

Naval Law Review

CONTROLLING THE USE OF FORCE IN CYBERSPACE: THE APPLICATION OF THE LAW OF ARMED CONFLICT DURING A TIME OF FUNDAMENTAL CHANGE IN THE NATURE OF WARFARE
Commander Todd C. Huntley, JAGC, USN

UNITED STATES ENVIRONMENTAL LAW APPLIED IN THE ARCTIC OCEAN: FRUSTRATING THE BALANCE OF THE LAW OF THE SEA, NATIONAL SOVEREIGNTY, AND INTERNATIONAL COLLABORATION EFFORTS
Lieutenant Commander Joan M. Malik, JAGC, USN

THE SHIPBOARD PANDORA'S BOX: THE OPERATIONAL REALITY THAT AN EXPECTATION OF PRIVACY EXISTS IN ELECTRONIC COMMUNICATIONS ABOARD NAVAL VESSELS
Lieutenant Colonel Leon James Francis, USMC

FEDERAL COURT OR MILITARY COMMISSION: THE LEGAL DILEMMA POSED BY THOSE CHARGED WITH TERRORIST VIOLENCE
Colonel James P. Terry, USMC (Ret.)

RETIRING A "POLLUTING" FLEET: THE UNIQUE LEGAL CHALLENGES AND ENVIRONMENTAL HURDLES TO SUISUN BAY NON-RETENTION VESSEL DISPOSAL
Lieutenant Ryan M. Anderson, JAGC, USN

TOWARD A NEW BEGINNING WITH THE INTERNATIONAL CRIMINAL COURT
Lieutenant Jeremy L. Snellen, JAGC, USN

WHEN RUF GETS ROUGH IT LOOKS LIKE R2P: COMPARING MICRO-LEVEL RULES FOR USE OF FORCE IN POST-CONFLICT COUNTRIES CHALLENGED BY ETHNIC, TRIBAL, AND CULTURAL VIOLENCE TO MACRO-LEVEL CONCEPTS OF HUMANITARIAN INTERVENTION AND RESPONSIBILITY TO PROTECT
Lieutenant Commander Scotch Perdue, JAGC, USN

Book Reviews

THE LIMITS OF POWER: THE END OF AMERICAN EXCEPTIONALISM
Major Scott A. DiRocco, USA

WIRED FOR WAR: THE ROBOTICS REVOLUTION AND CONFLICT IN THE 21ST CENTURY
Major Robert A. Rodrigues, USA



VOL. 60

THE NAVAL LAW REVIEW

2010

VOL. 60

2010

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 2010		2. REPORT TYPE		3. DATES COVERED 00-00-2010 to 00-00-2010	
4. TITLE AND SUBTITLE Naval Law Review, Vol. 60				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Law Review, Naval Justice School, 360 Elliot Street, Newport, RI, 02841				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 236	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

SUBSCRIPTIONS

Subscription information may be obtained by writing to the Managing Editor, NAVAL LAW REVIEW, Naval Justice School, 360 Elliot Street, Newport, RI 02841-1523. Publication exchange subscriptions are available to organizations that publish legal periodicals.

INDIVIDUAL PURCHASES

Individual copies of the Naval Law Review, formerly titled the *JAG Journal*, may be purchased by contacting the Defense Technical Information Center (DTIC) and the National Technical Information Service (NTIS) for republication and sale. Copies are not available from the Naval Justice School.

Commands not already registered with the DTIC may obtain registration forms and information on ordering publications by writing to:

Defense Technical Information Center
Attention: Code DTIC-FDRA
Cameron Station, Building 5
Alexandria, VA 22304-6145
COMM (703) 767-8273
DSN 427-8273
1-800-CAL-DTIC (225-3842)

Individual purchasers may obtain information on ordering publications by writing to:

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161

CONTENTS

Articles, Essays & Notes

CONTROLLING THE USE OF FORCE IN CYBERSPACE: THE APPLICATION OF THE LAW OF ARMED CONFLICT DURING A TIME OF FUNDAMENTAL CHANGE IN THE NATURE OF WARFARE <i>Commander Todd C. Huntley, JAGC, USN</i>	1
UNITED STATES ENVIRONMENTAL LAW APPLIED IN THE ARCTIC OCEAN: FRUSTRATING THE BALANCE OF THE LAW OF THE SEA, NATIONAL SOVEREIGNTY, AND INTERNATIONAL COLLABORATION EFFORTS <i>Lieutenant Commander Joan M. Malik, JAGC, USN</i>	41
THE SHIPBOARD PANDORA’S BOX: THE OPERATIONAL REALITY THAT AN EXPECTATION OF PRIVACY EXISTS IN ELECTRONIC COMMUNICATIONS ABOARD NAVAL VESSELS <i>Lieutenant Colonel Leon James Francis, USMC</i>	93
FEDERAL COURT OR MILITARY COMMISSION: THE LEGAL DILEMMA POSED BY THOSE CHARGED WITH TERRORIST VIOLENCE <i>Colonel James P. Terry, USMC (Ret.)</i>	125
RETIRING A “POLLUTING” FLEET: THE UNIQUE LEGAL CHALLENGES AND ENVIRONMENTAL HURDLES TO SUISUN BAY NON-RETENTION VESSEL DISPOSAL <i>Lieutenant Ryan M. Anderson, JAGC, USN</i>	141
TOWARD A NEW BEGINNING WITH THE INTERNATIONAL CRIMINAL COURT <i>Lieutenant Jeremy L. Snellen, JAGC, USN</i>	167
WHEN RUF GETS ROUGH IT LOOKS LIKE R2P: COMPARING MICRO-LEVEL RULES FOR USE OF FORCE IN POST-CONFLICT COUNTRIES CHALLENGED BY ETHNIC, TRIBAL, AND CULTURAL VIOLENCE TO MACRO-LEVEL CONCEPTS OF HUMANITARIAN INTERVENTION AND RESPONSIBILITY TO PROTECT <i>Lieutenant Commander Scotch Perdue, JAGC, USN</i>	189

Book Reviews

- THE LIMITS OF POWER: THE END OF AMERICAN EXCEPTIONALISM 215
Major Scott A. DiRocco, USA
- WIRED FOR WAR: THE ROBOTICS REVOLUTION AND CONFLICT IN
THE 21ST CENTURY 223
Major Robert A. Rodrigues, USA

CONTROLLING THE USE OF FORCE IN CYBER SPACE: THE APPLICATION OF THE LAW OF ARMED CONFLICT DURING A TIME OF FUNDAMENTAL CHANGE IN THE NATURE OF WARFARE

Commander Todd C. Huntley¹

*"America's failure to protect cyber space is one of the most urgent national security problems facing the country."*²

I. INTRODUCTION

Cyber attacks against U.S. government systems, critical infrastructure, and private networks are now reported in the media on an almost daily basis. The threat posed to U.S. national security by these attacks, as well as U.S. government efforts to defend against them, have also received much attention lately. One of President Obama's first acts upon taking office was to order a comprehensive 60-day review of U.S. cyber space policy.³ In April 2009 Congress introduced three different bills addressing various aspects of cyber security.⁴

While the threat to U.S. national security posed by cyber intrusions and attacks is widely discussed in both the government as well as the media, the U.S. continues to struggle to develop a cyber security strategy.⁵ These discussions, as

¹ Judge Advocate General's Corps, United States Navy. Currently serving as the Staff Judge Advocate for Commander, Special Operations Command Central and Combined Forces Special Operations Component Command. B.A., 1991, University of Cincinnati; J.D., 1996, University of Cincinnati; M.A., 2006, Fletcher School of Law and Diplomacy; L.L.M., 2009, Harvard Law School. The views expressed in this article are those of the author and do not represent the views of the Department of Defense or Department of the Navy. All information obtained for this article was gathered from unclassified sources. The author would like to thank Professor Jack Goldsmith for his invaluable assistance and advice.

² S. 773, 111th Cong. (2009).

³ White House Press Statement, *President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review* (Feb. 9, 2009) available at http://www.whitehouse.gov/the_press_office/advisorstoconductimmediatecybersecurityreview/.

⁴ Ben Bain, *Lawmakers Attack Cybersecurity on Multiple Fronts*, FEDERAL COMPUTER WEEK, May 1, 2009, available at <http://www.fcw.com/Articles/2009/05/04/news-congress-cybersecurity.aspx>.

⁵ The existing National Strategy to Secure Cyber space was published in February 2003 and is widely seen as inadequate to deal with current threats to critical U.S. infrastructure, systems and networks. See NATIONAL RESEARCH COUNCIL, *Technology, Policy, Law, and Ethics Regarding*

highlighted by the President's 60-day review, the recently introduced bills, and recent media reports, have focused almost solely on what measures must be taken to improve the nation's cyber defenses. With the exception of a recently published report by the National Research Council, there has been no public discussion of U.S. offensive cyber strategy.⁶

This report is also one of the first documents to make the distinction that, despite the widespread use of the terms "cyber warfare" and "cyber attack," most of the cyber activity targeting U.S. systems are not, under the existing law of armed conflict, attacks at all.⁷ If the individual malicious act does not rise to the level of an "attack," then it would seem to logically follow that the U.S. is not the target of a broader "cyber warfare" campaign, yet these terms continue to be used to describe the thousands of cyber intrusions that target U.S. critical infrastructure, systems and networks every day.

The U.S. economy, social life, and government, including national security has become intertwined with, and dependent on, the Internet and the myriad of activities taking place in cyber space. Thus, U.S. national interests have expanded beyond keeping sea lanes open for trade and now also include keeping the pathways of cyber space open for the economic, social, and security interests of the country and its citizens. In order to do this, the U.S. must also conduct operations in cyber space. The traditional tools of pursuing national interests must also be available to use in cyber space. Espionage, diplomacy, covert action, and even military force are no less important in cyber space than they are in the physical domain.

This requires not only a comprehensive cyber strategy, but also policy and doctrine to guide actions in furtherance of that strategy.⁸ This will include an understanding of how the law of armed conflict, especially the *jus ad bellum* body of law, applies to these activities in cyber space. While many facets of the traditional law of armed conflict paradigm do apply, there are also aspects that do not and that are inadequate in either deterring hostile acts or in containing the potential escalation that could result from cyber attacks.

The majority of the cyber attacks targeted at the U.S. are, in fact, not attacks at all. Thus, the law of armed conflict has limited application in controlling these activities and the resulting harm. While domestic criminal law does make almost all of these activities illegal, enforcement of the law remains

U.S. Acquisition and Use of Cyber attack Capabilities (2009) available at http://books.nap.edu/openbook.php?record_id=12651&page=R1 [hereinafter NRC Report].

⁶ See *id.*

⁷ *Id.*

⁸ *Id.*

another matter.⁹ Given the relatively slim possibility of identifying the perpetrators, let alone apprehending them, domestic criminal law fails to serve as much of a deterrent to those carrying out these acts. The majority of the acts, particularly those that are state-sponsored or carried out by state actors, would also be a violation of state sovereignty. Of course, state sovereignty and international law does little to control the behavior of non-state actors; however, given the relative risk-gain analysis, these principles of international law also do little to control the conduct of states in cyber space.

International law, the law of armed conflict, and domestic criminal law do not adequately deter either states or non-state actors from using cyber attack and cyber intrusion capabilities to pursue their national and group interests in a manner harmful to the national interests of the U.S. Both states as well as non-state actors have much to gain from conducting cyber operations with relatively low risk given the relative ease with which these operations may be conducted anonymously, and the relatively dismal state of current cyber defenses.

Legal writing has tended to focus solely on state-on-state cyber warfare as part of a broader, more traditional, armed conflict, or that takes place solely in cyber space.¹⁰ There has been relatively little written about the application of existing legal regimes to persistent cyber attacks that fall below the level of an armed attack or use of force and the difficulty faced by states in responding to these attacks, and even less written about the offensive use of such cyber operations to further U.S. national interests.¹¹ Although the U.S. may be the nation most vulnerable to cyber attacks, it also has much to gain from offensive cyber operations, and must carefully consider any changes to existing legal regimes that may further limit such activity. Existing legal regimes fail to provide adequate guidance both to U.S. responses to cyber attacks as well as U.S. offensive cyber operations.

II. DEFINING AND CHARACTERIZING CYBER ACTIVITY

The terms “cyber warfare” and “cyber attack” are commonly used to refer to all unauthorized cyber activity, regardless of the nature of the activity,

⁹ See Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (1984).

¹⁰ See Knut Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks*, at [http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/68LG92/\\$File/ApplicabilityofIHLtoCNA.pdf](http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/68LG92/$File/ApplicabilityofIHLtoCNA.pdf) (last visited Mar. 26, 2010); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999) [hereinafter Schmitt, *CNA*]; Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, IRRC Vol. 84, No. 846 (June 2002), available at [http://www.icrc.org/Web/eng/siteeng0.nsf/3e02cd6224ce0af6012568b20048a62f/e4e4a03de3be1211c1256bf900332f62/\\$FILE/365_400_Schmitt.pdf](http://www.icrc.org/Web/eng/siteeng0.nsf/3e02cd6224ce0af6012568b20048a62f/e4e4a03de3be1211c1256bf900332f62/$FILE/365_400_Schmitt.pdf) [hereinafter Schmitt, *Wired Warfare*].

¹¹ See NRC Report, *supra* note 5.

who is conducting the activity, or the consequences which result from the activity. Distributed denial of service “attacks,” extraction or modification of information, website vandalism, as well as insertion of malicious code designed to damage, or destroy, data and systems, are all referred to as “cyber attack” or even “cyber warfare” regardless of whether these activities result in death, destruction of property, or merely the loss of information. Intrusions and other activity conducted by disgruntled employees, teen-age hackers, and criminals, are typically not distinguished from those by terrorists or foreign intelligence and military personnel.¹²

Overbroad use of the terms “cyber attack” and “cyber warfare” and a failure to clearly define the various cyber capabilities also creates problems for the development of policy and doctrine for the use of these capabilities, as well as adding difficulty in developing a response to such activities. How an activity or capability is defined will often determine the authority for conducting that activity or using that capability. This may also determine which personnel have authority to conduct the activity, including which Executive agency will conduct the activity as well as who will be responsible for the oversight of the activity. Such oversight would include not only oversight bodies within the Executive branch, but also which Congressional committee(s) will have oversight responsibilities. Perhaps even more importantly, how an activity or capability is classified will determine which appropriated funds may be used for the purchase of equipment and tools, the payment of personnel conducting the activity, and the research and development of tools and capabilities.

Current U.S. Department of Defense (“DoD”) doctrine refers broadly to cyber operations as Computer Network Operations (“CNO”).¹³ CNO is one of the core capabilities of Information Operations (“IO”) along with electronic warfare, psychological operations, military deception and operations security.¹⁴ U.S. doctrine further subdivides CNO into three different categories; Computer Network Defense (“CND”), Computer Network Attack (“CAN”), and Computer Network Exploitation (“CNE”). CND has received the most attention in terms

¹² This failure to distinguish between more and less destructive activity as well as between thrill-seekers, criminals and those with hostile intent may be due as much to the difficulty in determining these things as it is to any other reason. *See id.*

¹³ CNO is not defined as a separate activity, but only as “[c]omprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.” DEP’T OF DEFENSE, JOINT PUBLICATION 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, Apr. 12, 2001, as amended through Oct. 17, 2008, *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf [hereinafter JP 1-02].

¹⁴ Information Operations is defined by the DoD as “[t]he integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.” *Id.*

of public discourse and is defined by DoD as “[a]ctions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the DoD information systems and computer networks.”¹⁵

CNA is defined by DoD as “[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.”¹⁶ Thus, the target of a CNA may be not only the physical, i.e., the hardware, but also the information stored on, or transiting through, the systems and networks. When this definition is examined in more detail, it is apparent that it encompasses effects that would constitute a use of force, or possibly even an armed attack, i.e., the destruction of computers and computer networks, as well as effects that fall under this threshold, i.e., the disruption or denial of information.¹⁷ Thus, even this official DoD definition is too broad to have any meaningful use in conducting a legal review of activities termed CAN, and lawyers doing so will have to review the cyber tool being employed, the method in which it is being employed, and the likely effects to determine whether the activity will be considered as a use of force, an armed attack, or perhaps some other type of unlawful activity.

CNE is defined by DoD as “[e]nabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.”¹⁸ CNE is probably the cyber activity that is least publicly discussed, but also very likely the activity most widely conducted, as evidenced by many of the intrusions reported in the media. Like the case of CNA, the official DoD definition of CNE actually refers to two very different activities. The first, “enabling operations,” refers to the preparatory steps necessary to gain access to target systems and networks.¹⁹ This activity is not conducted to obtain substantive intelligence; rather, it is to gain information that will then be used to conduct a CNA against the system or network at some point in the future. The other activity included in the definition is designed to gather substantive intelligence that is resident on the systems and networks, or that can be obtained through the targeted systems and networks.²⁰

Whether an activity is considered CNE or CNA is often the subject of great debate between the organizations with responsibility for those different

¹⁵ JP 1-02, *supra* note 13.

¹⁶ *Id.*

¹⁷ Daniel Silver, Computer Network Attack as a Use of Force Under Article 2(4), 76 INT’L. STUD. 73, 92–93 (2002).

¹⁸ JP 1-02, *supra* note 13.

¹⁹ *Id.*

²⁰ *Id.*

activities. Organizational turf battles account for some of the disagreement over the characterization of the various cyber activities, as the U.S. Intelligence Community will usually control CNE resources while the DoD will usually control CNA resources.²¹

There are also operational issues associated with how cyber activities are characterized. Which organizations have authority to conduct the activity, which appropriated funds may be used to pay for the resources and operations, what oversight procedures apply to the activity, and which approval procedures must be used will have to be determined according to how the activity is characterized. This situation leads to delay. Lawyers give incorrect advice, commanders are hesitant to use capabilities, and plans are disapproved because of policy and doctrine that does not adequately consider new technologies and capabilities.

This problem also exists when cyber capabilities are used as part of broader military activities such as military deception and psychological and counter-intelligence operations. Questions regarding who must approve the operation and what limitations apply, e.g., must the doctrine and policy for each separate activity be followed or does the primary purpose of the activity dictate which procedures govern, create confusion and delay. Much of this is a result of a lack of thinking about how new cyber technologies may be used across the spectrum of military operations. While cyber attack comprises only a small portion of a much broader area of cyber operations, little attention is typically paid to the relationship between cyber attack and other cyber capabilities or how these various cyber capabilities may be developed as part of a broader cyber activity strategy and policy.²²

Overbroad use of these terms may also force the application of the law of armed conflict regime when it may not necessarily apply. This has both offensive and defensive implications. Acts termed as “cyber attack” but which do not reach the threshold of an armed attack or use of force may unnecessarily be taken off the table as offensive options. Conversely, declaring acts against your own systems and networks as “cyber attacks” may lead to an unlawful response and an escalation of force. This is especially important in the case of cyber activities because, if the law of armed conflict is going to be applied by analogy, then terms must be used consistently and “cyber attack” should be used only to describe those operations that are equivalent to a use of force or armed attack. Thus it is important to be clear in the use of terminology to describe the malicious cyber activity and to understand the legal regime that would apply to that activity.

²¹ See NRC Report, *supra* note 5, at Box 3-2, for an introduction to this structural issue.

²² NRC Report, *supra* note 5, at 3-5.

This article will use the term “cyber activities” to refer to the entire spectrum of activities that states and their agents conduct in cyber space, i.e., in a manner roughly equivalent to the DoD doctrinal term “computer network operations.” “Cyber activities” would include defensive response actions, offensive cyber attack, and cyber espionage. Although not specifically addressed in this paper, this term would also encompass cyber facilitated Information Operation capabilities such as psychological operations and military deception.

The term “cyber attack” will be used to refer to those cyber activities with consequences or effects equivalent to a use of force or armed attack. These acts may be purely offensive in nature or they may also be in response to an attack, i.e., self-defense. The term “cyber warfare” will be used to refer to a series of sustained and coordinated “cyber attacks.” Both “cyber attacks” and “cyber warfare” can take place as part of a broader armed conflict or can be limited to a conflict taking place only in cyber space. “Cyber intrusion” will be used to refer to any unauthorized access to a database, computer, computer system, or network, regardless of the effect or consequence of such access. Thus, almost all “cyber activities,” and certainly all “cyber attacks,” will begin with a “cyber intrusion.” The most common “cyber intrusion” will be those conducted to collect information or intelligence, i.e., “cyber espionage.”

III. OVERVIEW OF THE THREAT: RECENT CYBER ATTACKS AND INTRUSIONS

Reports of new cyber intrusions are now reported in the media on an almost daily basis and, it is likely that, because of the highly sensitive nature of many of these, that most intrusions are never reported publicly.²³ While many attempted intrusions are detected and prevented, many are never detected and are successful in penetrating networks and systems of government agencies and private organizations across the country. The threat posed by these undetected intrusions was put rather simply in a recent speech by the head of U.S. counter-intelligence, Joel Brenner, who stated, “I worry more about the attacks we can’t even see.”²⁴ This section will briefly discuss some of the more recent, and well-known, intrusions that have been discovered.

Despite the growing attention given to many of these intrusions, such activity is not a recent development. At least as early as 1998, DoD networks

²³ Dr. Joel F. Brenner, Nat’l Counterintelligence Exec., 4th Annual Multi-Interest Conference, Institute for Defense and Government Advancement, Vienna, VA (Feb. 24, 2009), *available at* http://www.dni.gov/speeches/20090224_speech.pdf [hereinafter Brenner remarks].

²⁴ Bill Gertz, *China Blocks U.S. from Cyber Warfare*, WASHINGTON TIMES, May 12, 2009, *available at* <http://washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/print/>.

were targeted by cyber intrusions in an incident referred to as Solar Sunrise.²⁵ This activity was “widespread, systematic and showed a pattern that indicated they might be the preparation for a coordinated attack on the Defense Information Infrastructure.”²⁶ While the U.S. government originally believed Iraq to be behind these intrusions, in reality it was the work of teenagers from Israel and California.²⁷ Those responsible for these intrusions gained access to DoD computer systems around the world, left a program that would collect data from the system, and then later returned to retrieve that data.²⁸ Further information on what data was collected or what other activity was conducted, if any, has not been released.²⁹ By the end of this incident, over 500 systems were compromised in this series of intrusions and included not only military systems but also commercial and educational systems.³⁰ These intrusions confirmed what many within the government had been thinking: that DoD computer systems are vulnerable to attack even by those with very limited resources.³¹

Another series of early cyber intrusions into sensitive DoD, Department of Energy, NASA, and defense contractor computer systems was referred to as Moonlight Maze.³² This series of intrusions, which occurred over the period of a year from 1998 to 1999, were well coordinated and appeared to originate from Russia, although the involvement of the Russian government could never be proven.³³ These intrusions siphoned off an extremely large amount of information and, in some cases, installed a trapdoor in order to gain access again at a later date.³⁴ This series of incidents appeared to be designed to gain access to systems in order to extract information and not to damage or destroy the systems or networks themselves.

In a 2009 speech to the Council on Foreign Relations, New York Police Commissioner Raymond Kelly reported that a network of hackers has been making as many as 70,000 attempts a day to gain access to NYPD computer

²⁵ ANTHONY H. CORDESMAN, CYBER-THREATS, INFORMATION WARFARE AND CRITICAL INFRASTRUCTURE PROTECTION 40-41 (2002); *see also*, John J. Hamre, Deputy Secretary of Defense to the House Armed Services Committee on Defense Information Superiority and Information Assurance – Entering the 21st Century, Statement, Feb. 23, 1999, *available at* http://www.fas.org/irp/congress/1999_hr/99-02-23hamre.htm [hereinafter Hamre Statement]; CNN Online, Hackers Target Pentagon Computers, <http://www.cnn.com/US/9903/05/pentagon.hackers/index.html> (last visited Feb. 25, 2010).

²⁶ Hamre statement, *supra* note 25.

²⁷ Kevin Poulsen, *Solar Sunrise Hacker ‘Analyzer’ Escapes Jail*, THE REGISTER, Jun.15, 2001, *available at* http://www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_analyzer_escapes/.

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Id.*

³¹ Hamre statement, *supra* note 25.

³² CORDESMAN, *supra* note 25, at 39.

³³ *Id.*

³⁴ *Id.*

systems.³⁵ The Department identified these attempts as coming from IP addresses in China, the Ukraine, and the Netherlands, with the greatest number coming from China.³⁶ Kelly claimed that the hackers had yet to be successful, but that the attempts have forced the Department to increase its defensive efforts.³⁷ While Kelly surmised that the Department may be targeted by hackers because of its extensive international connections and counter-terrorist efforts, he did not elaborate on the nature of the activity or what he believed was the purpose of the attempted intrusions.³⁸

In addition to being subject to targeted intrusions like those discussed above, systems and networks also remain vulnerable to being infected with viruses. One such case was a recent infection of French Navy systems by the Conficker virus.³⁹ This infection prevented French naval aircraft from downloading flight plans and grounded the planes until a work around could be developed.⁴⁰ The infection forced the French Navy to sever links with outside networks and to rely on mail, faxes, and telephones as means of communication until the virus was eliminated.⁴¹ French naval officials believed that the infection was not a deliberate attack, but was most likely the result of someone using an infected USB device and a failure to update security patches.⁴² According to reports, the British Ministry of Defence was also affected by the virus, which infected computers at a large number of Royal Air Force bases and seventy-five percent of the Royal Navy fleet.⁴³

Recent reports revealed that the computer systems of the Tucson Police Department were infected, forcing the Department to disconnect its system from national crime databases.⁴⁴ Although the virus did not disrupt emergency services, future infections certainly could wreak havoc by shutting down communications, affecting emergency responses and communications.⁴⁵ It is not unfathomable that a terrorist organization could carry out a similar

³⁵ Alison Gendar and Bill Hutchinson, *International Hackers, Many from China, are Attacking NYPD Computers*, NEW YORK DAILY NEWS, Apr. 22, 2009, available at http://www.nydailynews.com/news/2009/04/22/2009-04-22_international_hackers_lauching_attack_against_nypd_computers.html.

³⁶ *Id.*

³⁷ *Id.*

³⁸ *Id.*

³⁹ Kim Willsher, Telegraph.co.uk, French fighter planes grounded by computer virus, <http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html> (last visited Feb. 26, 2010).

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.*

⁴⁴ Eric Sagara, *Tucson Police Department battling computer viruses*, TUCSON CITIZEN, Apr. 22, 2009, available at <http://www.tucsoncitizen.com/daily/local/114967.php>.

⁴⁵ *Id.*

operation, bringing down emergency communication systems immediately prior to a terrorist attack or doing so merely to induce panic. It is foreseeable that criminal organizations might also undertake such an operation in order to facilitate some other criminal activity such as a bank robbery.

Such infections may indeed be the result of a targeted infection or perhaps are infected unintentionally as a result of careless operators. Often, how the infection occurred is not reported or may not be ascertainable. Computer virus infections occur at an alarming rate and are typically viewed with little suspicion. Terrorists, criminal organizations, and foreign intelligence services might choose this technique of cyber attack or intrusion in order to divert attention away from their actual intent. This technique again reflects the difficulty in determining the intent behind many cyber activities, particularly when the source of the activity cannot be attributed. Regardless of whether these infections are intentional or unintentional, they threaten the safety of communities and may also threaten national security.

Another disturbing series of cyber intrusions was those directed at the networks of U.S. Central Command, the command responsible for directing the wars in Iraq and Afghanistan.⁴⁶ This attack led to the U.S. DoD banning the use of flash drives and other USB media and the increase in the information security level, or INFOCON. While the DoD did not release much information on the nature of the intrusion or what, if any, information had been compromised, it was reported that systems in Iraq and Afghanistan were accessed. This intrusion also highlights what is perhaps the biggest vulnerability in network and system security, the human operator. It is not known why infected USB media was chosen as a delivery mechanism for the software, but such a technique would allow an adversary to gain access to systems through which he is unable to gain technical access from outside the network.

Another series of intrusions that has recently been reported by the media was those that took place into the networks of DoD contractors building the newest Air Force fighter aircraft, the F-35 Joint Strike Fighter ("JSF").⁴⁷ Initial reports claimed that several terabytes of information on the aircraft's design and electronics systems had been downloaded but that the most sensitive information had not been accessed, as it is stored on systems not connected to the Internet.⁴⁸ This intrusion also gained access to Air Force air traffic control

⁴⁶ Julian E. Barnes, *Cyber-attack on Defense Department computers raises concerns*, LOS ANGELES TIMES, Nov. 28, 2008, available at <http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28>.

⁴⁷ Siobhan Gorman, August Cole, and Yochi Dreazen, *Computer Spies Breach Fighter-Jet Program*, WALL STREET JOURNAL, Apr. 21, 2009, available at <http://online.wsj.com/article/SB124027491029837401.html>.

⁴⁸ *Id.*

systems and allowed the hackers to view the location of Air Force aircraft.⁴⁹ This sophisticated intrusion encrypted the information as it was taken so that it was impossible to identify what information had been stolen.⁵⁰

Investigators were fairly certain, based on the IP addresses used in the intrusions and with other digital evidence, that the intrusions originated in China.⁵¹ These intrusions illustrate the difficulty in securing systems that are vital for national security as they are only as good as the weakest link, and when much of the information is stored on systems operated and owned by private defense contractors, the government's ability to secure these systems is limited.⁵² Air Force officials and others have recently claimed that the intrusions into these systems have been exaggerated and that only maintenance-related information was compromised.⁵³ Again, there has been little information released on these intrusions, with the Air Force refusing to confirm or deny any reports on the nature of the information that was compromised, only acknowledging that intrusions occurred.⁵⁴ An Air Force spokesman stated, "[i]n general, we don't comment on alleged or actual cyber infiltrations ... because any information we release ... could assist people in planning and executing future attacks."⁵⁵

This intrusion is likely to be the kind of malicious cyber activity with which the U.S. is faced in the future. Information on the technical capabilities of U.S. weapons systems would allow an adversary to counter the technological advantage currently enjoyed by the U.S. and possibly defeat these systems on the battlefield. Additionally, such information would allow adversaries to improve their own weapons systems by copying the technology stolen from the U.S. While such activity may not present an immediate threat to the national security of the U.S. such as that posed by kinetic, physical attacks or cyber attacks that result in destruction of systems and networks, the long-term threat could be even greater.

Perhaps the most troubling of the recent intrusions reported in the media was the compromise of systems linking the U.S. power grids.⁵⁶ Officials reported that these intrusions came primarily from China and Russia and were

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² Gorman, *Computer Spies Breach Fighter-Jet Program*, *supra* note 47.

⁵³ Eric Holmes, *Officials: Cyber attack Not That Damaging*, AIR FORCE TIMES, Apr. 26, 2009, available at http://www.airforcetimes.com/news/2009/04/airforce_cyberspies_042509/.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ Siobhan Gorman, *Electricity Grid Penetrated by Spies*, WALL STREET JOURNAL, Apr. 8, 2009, available at <http://online.wsj.com/article/SB123914805204099085.html>.

conducted in order to map out the U.S. electrical system and to implant software that could be activated in the future to shut down these systems or destroy parts of the electrical system infrastructure.⁵⁷ Based on the sophistication of the intrusions, it appears that these attacks were most likely conducted by China and Russia.⁵⁸ While these intrusions have not damaged the systems, they could be used to do so during a time of conflict or at some time in the future.⁵⁹ In addition to the electrical system, it appears that other infrastructure components such as sewage and water systems were also targeted.⁶⁰

The Wall Street Journal reported that these intrusions were not detected by the organizations controlling the targeted infrastructure components but rather were detected by U.S. intelligence agencies.⁶¹ A CIA official had reportedly stated that power equipment had been “taken out” some time in 2008 and that this had been followed by demands for money.⁶² This report also claimed that DoD has spent over \$100 million in the past six months to repair damage inflicted by cyber intrusions into DoD systems and networks.⁶³ This type of intrusion is perhaps the most troublesome as, although the initial activity, i.e., gaining access to the system, is similar in appearance to the others mentioned above, it carries with it consequences that potentially could be equivalent to those caused by the use of kinetic force.

The cyber intrusions discussed above highlight the fundamentally different nature of the cyber threat. Out of the several examples mentioned, it appears that in only one case were those responsible affirmatively identified and held responsible. Although in several of the examples investigators identified the general geographic location from where they believed the malicious activity emanated, there was no way to tell for certain whether this was, in fact, the location or whether the activity had merely been routed through that location in an effort to shift blame or throw off investigators. This uncertainty in attribution of malicious cyber activity is perhaps one of the most difficult issues facing those working in this area, and will be discussed in more detail later in this article.

The examples discussed also highlight the ease with which individuals may gain access to sensitive and valuable information. They gained access through interconnected systems and networks, as well as exploited human security weaknesses by using portable media devices to gain access to U.S.

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ *Id.*

⁶⁰ *Id.*

⁶¹ Gorman, *Electricity Grid Penetrated by Spies*, *supra* note 56.

⁶² *Id.*

⁶³ *Id.*

military computers. These examples, along with the numerous others reported in the media, demonstrate that the very nature of the Internet which has made it a vital part of the U.S. and global economies, i.e., its capability to connect people in a manner like none other before it, is also its Achilles heel. Access to the U.S. power grids, local police departments, defense contractors, and U.S. military computers in Iraq and Afghanistan can be obtained from anywhere else in the globe and, to top it off, that access can be made to appear as if it came from somewhere else.

Finally, the example of the intrusions into the U.S. power grids shows just how difficult it is to detect cyber intrusions. In the case discussed above, the victims of the intrusion were unaware their systems had been compromised and remained so until the intrusions were detected by the intelligence community. This example also illustrates what may be the greatest challenge to defending against, and responding to, the threat posed by cyber attacks and cyber intrusions - that is, once an intrusion has been detected, the inability to determine the intent of those responsible for the intrusion or its likely consequences. Individuals gain access to systems and networks for many different reasons: teen-age pranks, criminal blackmail, corporate and state espionage, and possibly to cause physical destruction. Lacking the capability to determine the intent of the perpetrator makes it almost impossible to structure an appropriate, lawful response, and is likely to leaving a state guessing as to whether it was facing an imminent cyber attack or merely a teen-ager taking the family computer out for a spin.

IV. CYBER WARFARE AND THE LAW OF ARMED CONFLICT

The development of cyber warfare capabilities presents yet another challenge to the application of the law of armed conflict to modern conflicts and 21st century threats.⁶⁴ While the basic principles of the law of armed conflict have proven remarkably adaptable to the development of new weapons and methods of warfare in the past, the strategic threat posed by cyber intrusions has resulted in a fundamental shift in the nature of warfare.⁶⁵ In particular, the *jus ad bellum* paradigm as currently structured is inadequate in containing and responding to the strategic threat posed by cyber capabilities to U.S. national security as well as broader international peace and security.⁶⁶

⁶⁴ Reference to the law of armed conflict generally includes both *jus in bello*, principles designed to limit suffering and destruction once an armed conflict has begun, and *jus ad bellum*, principles governing when a state may legitimately use force. This paper uses the term "law of armed conflict" in this broader sense to include both *jus ad bellum* and *jus in bello* principles. The terms *jus ad bellum* and *jus in bello* will be used when referring specifically to those specific legal regimes.

⁶⁵ See Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L. J. 179, 179-181 (2006).

⁶⁶ See Schmitt, CNA, *supra* note 10.

Most writers agree that *jus in bello* applies to cyber attacks that take place as part of an armed conflict, as well as to those cyber activities which themselves are considered to be a use of force.⁶⁷ The principles of military necessity, distinction, and proportionality would all apply to those cyber attacks which cause effects similar to those caused by a kinetic use of force, i.e., injuries, death, or destruction of property.⁶⁸ The application of the law of armed conflict by analogy however begins to break down when a *jus ad bellum* analysis is applied to cyber activity.⁶⁹

While some scholars have examined the legal challenges presented by cyber warfare, they have mostly focused on the application of the law of armed conflict to state-on-state cyber warfare or the application of domestic criminal law to cyber intrusions conducted by individuals. The challenge to existing legal regimes posed by cyber activities that do not rise to the level of a use of force or an armed attack, as well as the challenge presented by the largely unattributable nature of most cyber attacks and cyber intrusions, remains largely unexamined and, in my opinion, represent two of the most fundamental issues that need to be addressed in developing both a comprehensive cyber security strategy as well as a legal regime that will apply to cyber attacks and cyber intrusions.

This section of the article will examine the existing *jus ad bellum* paradigm and its application to cyber activity. It will discuss current approaches in the analysis of, and application to, *jus ad bellum* as well as proposed approaches in applying *jus ad bellum* to cyber activity.

⁶⁷ See Dörmann, *supra* note 10; Schmitt, *Wired Warfare*, *supra* note 10; Michael N. Schmitt, Heather A. Harrison, and Thomas C. Wingfield, *Computers and War: The Legal Battlespace*, Program on Humanitarian Policy and Conflict Research, Harvard University, June 2004, available at <http://www.ihlresearch.org/ihl/pdfs/schmittetal.pdf>; DEPARTMENT OF DEFENSE GENERAL COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (1999), available at <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf> [hereinafter DoD OGC Memo].

⁶⁸ See Dörmann, *supra* note 10; Schmitt, *Wired Warfare*, *supra* note 10; Schmitt et. al., *Computers and War*, *supra* note 67; DoD OGC Memo, *supra* note 67.

⁶⁹ See Duncan B. Hollis, *New Tools, New Rules: International Law and Information Operations, The Message of War: Information, Influence, and Perception in Armed Conflict*, Sep. 11, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1009224.

A. Overview of *jus ad bellum*

The body of *jus ad bellum* is found in both customary international and international treaty law.⁷⁰ The primary modern source of *jus ad bellum* is the Charter of the United Nations. Article 2(4) of the Charter prohibits both the threat of force, as well as the use of force, stating “[a]ll members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.”⁷¹ Professor Michael Schmitt analyzes Article 2(4)’s language regarding the “territorial integrity or political independence” of a state as meaning not that uses of force which do not threaten the territorial integrity or political independence are permissible, but that for a use of force to be permitted, some authority for that use of force must be found within the U.N. Charter.⁷² This authority to use force would typically be found either in a United Nations Security Council Resolution invoking Chapter VII of the Charter or in Article 51, both of which will be discussed in more detail later.

Unfortunately, neither the Charter nor customary international law contains a clear delineation of what actions constitute a prohibited use of force. Armed attacks such as the invasion of a neighboring country or the use of kinetic force, such as bombs and artillery, are clearly illegal uses of force; however, lesser hostile acts may also be found to violate the prohibition against the use of force.⁷³ As is the case in many areas of international law, exactly what acts, short of an armed attack, constitute a use of force will likely remain largely unsettled given the lack of a body with the authority to make binding decisions on this issue, and will develop only over time with state practice.

Traditional thinking had been that, for an activity to constitute a prohibited use of force, the use of a weapon producing a kinetic effect was required.⁷⁴ The development of chemical and biological weapons challenged this thinking and expanded the concept of what was considered a use of force, focusing not on the weapon or tool used in the activity, but rather on the effect

⁷⁰ See, NRC Report, *supra* note 5, at 7-2; *Case Concerning Military and Paramilitary Activities in and Against Nicaragua*, Advisory Opinion, General List No. 70 (Jun. 27, 1986), available at <http://www.icj-cij.org/docket/files/70/6503.pdf> [hereinafter *Nicaragua v. U.S.*].

⁷¹ U.N. Charter art. 2, para. 4. The Charter also provides two exceptions to this ban on the use of force: when authorized by the U.N. Security Council pursuant to Chapter VII of the U.N. Charter, and in self-defense, as provided for in Article 51. These both will be discussed in more detail later.

⁷² Schmitt, *CNA*, *supra* note 10, at 901. For a discussion as to whether this language expands the scope of what would be considered to be a use of force, see WALTER GARY SHARP, *CYBERSPACE AND THE USE OF FORCE* 88-91 (Aegis Research Corp. 1999).

⁷³ See generally, *Nicaragua v. U.S.*, *supra* note 70.

⁷⁴ Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT’L L. & POL. 57, 72 (2001).

produced by the activity.⁷⁵ It is accepted today that activities which have consequences similar to those produced by weapons, that is, physical injury and death to persons, or damage and destruction to property, will be considered to be uses of force and are prohibited by both Article 2(4) and customary international law. This approach has been useful and has allowed the law of armed conflict to evolve and apply to new means and methods of warfare as they have developed. This approach also has limitations, though, as it provides little guidance for analyzing those acts which do not have effects similar to a kinetic attack, some of which may still be considered to be a prohibited use of force.⁷⁶

There are several other sources which may lend some clarity to what acts, short of an armed attack or which produce an effect equivalent to that produced by kinetic, physical force, would also qualify as a use of force. In *Nicaragua v. the United States*, the International Court of Justice (“ICJ”) held that the laying of mines by the U.S. in Nicaraguan territorial waters was a use of force and a violation of the customary international law prohibition against the use of force.⁷⁷ The ICJ, finding that the prohibition against the threat or use of force contained in Article 2(4) generally reflects the same prohibition in customary international law, stated “by laying mines in the internal or territorial waters of the Republic of Nicaragua . . . the United States of America has acted . . . in breach of its obligations under customary international law not to use force against another State . . .”⁷⁸

In the *Nicaragua* case, the ICJ also examined the activities of the United States in providing various levels of support to the *contras* and found that those activities ranged from violations of the international legal principle of non-intervention to violations of the prohibition on the use of force. At one end was the provision of funds, with the court stating “that the mere supply of funds to the *contras*, while undoubtedly an act of intervention in the internal affairs of Nicaragua . . . does not in itself amount to a use of force.”⁷⁹ The court also examined the provision of more extensive logistical support, over and above funds, and held “that the support given by the United States . . . to the military and paramilitary activities of the *contras* in Nicaragua, by financial support, training, supply, of weapons, intelligence and logistic support, constitutes a clear breach of the principle of non-intervention.”⁸⁰

⁷⁵ *Id.*

⁷⁶ See *Nicaragua v. U.S.*, *supra* note 70.

⁷⁷ *Nicaragua v. U.S.*, *supra* note 70, at para. 147.

⁷⁸ *Id.*

⁷⁹ *Id.* at para. 228.

⁸⁰ *Id.* at para. 242.

The ICJ also examined a series of attacks on various facilities in Nicaragua and found that, although no U.S. personnel had executed the attacks complained of by Nicaragua, that “[a]gents of the United States participated in the planning, direction, support and execution of the operations” and that such acts constituted a use of force by the United States.⁸¹ While constituting a use of force by the United States, these acts did not rise to the level of an armed attack.

There appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks. In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also “the sending by or on behalf of a State of armed bands, groups, irregulars, or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to” (*inter alia*) an actual armed attack conducted by regular forces, “or its substantial involvement therein.”⁸²

Thus, “assistance to rebels in the form of the provision of weapons or logistical or other support . . . may be regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States,” but did not amount to an armed attack.⁸³

Guidance as to what acts might constitute a use of force may also be found elsewhere in the U.N. Charter and other international legal documents. Article 41 of the U.N. Charter specifically lists measures which are not considered to be a use of armed force, stating “[t]hese may include complete or partial disruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.”⁸⁴

Article 42 also gives further specific examples of acts that are considered to be uses of force, including “demonstrations, blockades, and other

⁸¹ *Id.* at paras. 81-86.

⁸² *Nicaragua v. U.S.*, *supra* note 70, at para. 195.

⁸³ *Id.*

⁸⁴ U.N. Charter art. 41:

The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.

operations by air, land, and sea forces”⁸⁵ Some coercive acts, while in a sense hostile, are also not to be considered as a use of force. During the drafting of the U.N. Charter, a group of developing countries wanted to include economic coercion as a prohibited act constituting a use of force.⁸⁶ This request was ultimately turned down.

It is helpful to think of the use of force analysis as taking place on a continuum, where armed attacks, the existence of which gives rise to a right to use force in self-defense, lie at one extreme, and where coercive but permissible acts such as economic coercion, “severance of diplomatic relations,” and “disruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication” lie at the opposite end of the continuum.⁸⁷ Those acts which fall in between are prohibited uses of force, but ones against which the victim state would not be permitted to use force in self-defense.

While the Charter prohibits states from threatening or using force to settle disputes, it also recognizes two different instances in which a state may use force. One such instance is when the use of force has been authorized by the U.N. Security Council pursuant to Chapter VII of the Charter.⁸⁸ If the Security Council has determined that a particular situation represents a threat to international peace and security pursuant to Article 39, it may impose measures not involving the use of force, as outlined in Article 41.⁸⁹ If these measures are inadequate, the Security Council, pursuant to Article 42, may authorize “operations by air, sea, or land forces of Members of the United Nations,” “as may be necessary to maintain or restore international peace and security.”⁹⁰

A state may also use force to defend itself and others against an armed attack. Article 51 of the U.N. Charter states: “Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an

⁸⁵ U.N. Charter art. 42:

Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.

⁸⁶ Barkham, *supra* note 74, at 70-71.

⁸⁷ See Schmitt, *CNA*, *supra* note 10, at 904.

⁸⁸ U.N. Charter, art 39.

⁸⁹ “The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.” U.N. Charter, art. 39. See also U.N. Charter, art 41.

⁹⁰ U.N. Charter, art. 42.

armed attack occurs against a Member of the United Nations”⁹¹ While Article 51 recognizes the use of force in individual or collective self-defense, the right to use force in self-defense is not dependent on a grant of authority by the Charter, but rather, is “inherent” and based in customary international law.⁹²

This right applies only to the use of force in self-defense against an armed attack and not to any lesser use of force other than an armed attack.⁹³ In *Nicaragua v. U.S.*, the United States argued that Nicaragua’s provision of arms to rebels in El Salvador constituted an armed attack against El Salvador, and that this armed attack justified the use of force, in this case laying mines in certain internal and territorial waters of Nicaragua.⁹⁴ The court disagreed and held that the provision of arms by Nicaragua to the rebels was a use of force, but did not rise to the level of an armed attack; thus, the U.S. was not entitled to use force in collective self-defense.⁹⁵ Thus, unlike Article 51, which allows for a remedy in the case of an armed attack, Article 2(4) offers no similar remedy to those states which are the targets of a use of force that falls below the level of an armed attack.⁹⁶

The ICJ opinion in the *Corfu Channel* case illustrates the potential danger for violating Article 2(4)’s prohibition on the use of force in responding to a provocative act.⁹⁷ The *Corfu Channel* case began when British warships passed through the channel and were fired upon by Albanian artillery.⁹⁸ Several months later, Britain again sent ships through the channel; however, this time, two of them struck mines. Following this incident, Britain sent armed minesweepers into Albanian territorial waters to clear the mines.⁹⁹

In the ensuing case, the ICJ held that the use of armed ships to sweep mines in Albanian waters was a violation of international law and was a “policy of force,” but did not find that this action was a violation of the Article 2(4) prohibition on the use of force. The court did find, however, that Albania’s use of artillery was a use of force and demonstrated the potential dangers in states

⁹¹ U.N. Charter, art. 51.

⁹² See, NRC Report, *supra* note 5, at 7.2.1.1.; DoD OGC Memo, *supra* note 67.

⁹³ “While an armed attack would give rise to an entitlement to collective self-defense, a use of force of a lesser degree of gravity cannot . . . produce any entitlement to take collective counter-measures involving the use of force.” *Nicaragua v. U.S.*, *supra* note 70, at para. 249.

⁹⁴ *Id.*

⁹⁵ *Id.* See also DoD OGC Memo, *supra* note 67, at 19.

⁹⁶ Schmitt, *CNA*, *supra* note 10, at 900.

⁹⁷ International Court of Justice, *The Corfu Channel Case* (Apr. 9, 1949), available at <http://www.icj-cij.org/docket/files/1/1645.pdf>. This danger is compounded in cyber space because of the attribution problems.

⁹⁸ *Id.*

⁹⁹ *Id.*

exercising self-help in such cases.¹⁰⁰ This case illustrates the potential dangers of using self-help to defend against, or respond to, a cyber attack or cyber intrusion.

Article 51, on its face, would seem to limit the use of force in self-defense only “if an armed attack occurs,” thus prohibiting the use of force in pre-emptive self-defense. If, however, the right to use force in self-defense referred to in Article 51 is really an inherent right grounded in customary international law, then pre-emptive, or anticipatory, self-defense is authorized in certain limited circumstances. The formal enunciation of the doctrine of anticipatory self-defense can be traced to the *Caroline* incident and was initially articulated by U.S. Secretary of State Daniel Webster, who stated that the use of force in anticipatory self-defense is appropriate where the need is “instant, overwhelming, and leav[es] no choice of means and no moment for deliberation.”¹⁰¹

The *S.S. Caroline*, which had been used to re-supply Canadian rebels, was burned and set adrift by Canadian loyalists and British naval personnel on December 29, 1837.¹⁰² In correspondence between Lord Ashburton and Daniel Webster, Webster argued that for the British destruction of the *Caroline* to be a legitimate act of self-defense, Britain would have to justify its actions by showing a “necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation.”¹⁰³ In the continuing correspondence, Ashburton accepted Webster’s statement of the law and proceeded to explain how the destruction of the *Caroline* was done in self-defense because it otherwise would have continued to supply rebels who were carrying out attacks.¹⁰⁴ Thus, in cases where an armed attack is imminent and there is no time in which to take other measures, a state would be authorized to use force in anticipatory self-defense.

The use of force in anticipatory self-defense is perhaps one of the most contentious issues in international law. Whether a state must first suffer an armed attack before responding with force in self-defense or whether it may use force first, in anticipation of an imminent attack, is a difficult question even

¹⁰⁰ *Id.*

¹⁰¹ The Avalon Project, Yale Law School, http://avalon.law.yale.edu/19th_century/br-1842d.asp (last visited Mar. 1, 2010).

¹⁰² *Id.*

¹⁰³ Letter from Daniel Webster, Secretary of State to Lord Ashburton, Jul. 27, 1842, *available at* http://avalon.law.yale.edu/19th_century/br-1842d.asp#web1 (last visited March 1, 2010).

¹⁰⁴ Letter from Lord Ashburton to Daniel Webster, Secretary of State, Jul. 28, 1842, *available at* http://avalon.law.yale.edu/19th_century/br-1842d.asp#ash1 (last visited Mar. 1, 2010).

when dealing with traditional, kinetic force. Determining what constitutes an imminent attack is even more difficult in the cyber realm.

B. Application of *jus ad bellum* to cyber attacks and intrusions

From almost the very first days of the Internet, the implications of cyber warfare have been contemplated by defense strategists and academics. Concomitant with the realization of the strategic potential of cyber warfare, lawyers began discussing how this new method of warfare would fit into the existing law of armed conflict regime. This debate has been ongoing for well over a decade, and yet there still has been no definite resolution as to which cyber activities constitute a use of force or how *jus ad bellum* principles will be applied to such activities.

Most observers agree that the law of armed conflict applies to cyber intrusions and cyber attacks.¹⁰⁵ The fact that cyber attack capabilities, or even the Internet itself, was not contemplated by the drafters of the Geneva and Hague Conventions does not place those activities outside the application of *jus in bello*. If a cyber activity rises to the level of a use of force or armed attack, then the principles of *jus in bello* would apply to that activity. The state conducting the cyber attack would be required to comply with the principles of military necessity, proportionality, distinction, and perfidy in its use of that capability and would be required to respect the rights of neutral nations. This general agreement should not be seen as an indication that the application of *jus in bello* to specific actions is simple or settled as a matter of law.

As is evidenced by the discussion above, even determining what “non-cyber” acts constitute a use of force, as well as what actions a state may take in response, is not well settled. This vast expanse of legal uncertainty has grown with the development of cyber capabilities and provides little concrete guidance as to what responses would be permissible or for states developing strategy for the offensive use of such capabilities.

In 1999 the DoD Office of General Counsel attempted to provide some guidance in this area, conducting a review and authoring an “assessment of international legal issues in information operations.”¹⁰⁶ This assessment was not limited to those legal issues related to cyber attacks or the use of force, but rather was a broad discussion of the many legal issues faced by military

¹⁰⁵ See NRC report, *supra* note 5, at 7-1.

¹⁰⁶ DoD OGC Memo, *supra* note 67.

commanders and operators as they plan, approve and conduct Information Operations.¹⁰⁷ The authors of the report highlighted this uncertainty, stating:

It is far from clear the extent to which the world community will regard computer network attacks as “armed attacks” or “uses of force,” and how the doctrines of self-defense and countermeasures will be applied to computer network attacks. The outcome will probably depend more on the consequences of such attacks than on their mechanisms. The most likely result is an acceptance that a nation subjected to a state-sponsored computer network attack can lawfully respond in-kind, and that in some circumstances it may be justified in using traditional military means in self-defense.¹⁰⁸

This “consequences” or “effects” approach to analyzing cyber activity as a use of force under *jus ad bellum* is a familiar one, as was discussed in the context of chemical and biological weapons above, and is the one favored by most observers today, including the DoD.¹⁰⁹

The challenges of applying the law of armed conflict paradigm to cyber attacks and intrusions is not limited just to identifying whether or not a specific activity is a use of force. States must also develop an analytical framework to determine what actions they may take in response to a cyber intrusion, as well as determine what responses their own actions will likely generate. The importance of this was addressed by the authors of the DoD report, stating:

An exploration of the manner in which international law on the use of force among nations is likely to apply to peacetime computer intrusions¹¹⁰ will serve three distinct purposes:
(1) it will enable a government that is resolved to conduct itself in scrupulous compliance with international law to avoid

¹⁰⁷ Information Operations is defined by the DoD as “[t]he integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.” JP 1-02, *supra* note 13.

¹⁰⁸ DoD OGC Memo, *supra* note 67, at 25. Given that U.S. government cyber operations, as well as the legal reviews of those operations, are highly classified, this report provided a rare insight into the interpretation and application of the law of armed conflict to DoD cyber operations.

¹⁰⁹ Other approaches will be discussed later in this article.

¹¹⁰ DoD OGC Memo, *supra* note 13. The term “peacetime computer intrusion” is not defined or explained further in the report. From the body of the report, it appears that this term is used to distinguish computer intrusions that occur during a broader, more traditional, armed conflict from those that occur in isolation from a use of kinetic armed force.

activities that are likely to be regarded by the target nation and the world community as violations of international law;
(2) it will enable a government contemplating activities that might be considered to violate international law to weigh the risks of such action;
(3) it will enable a government that is the victim of an information attack to identify the remedies afforded to it by international law, including appeals to the Security Council, the use of force, and other self-help remedies not involving the use of force.”¹¹¹

Thus, understanding the application of *jus ad bellum* principles to computer intrusions which occur outside of a traditional armed conflict is important for understanding the implications of both offensive and defensive applications of cyber intrusions, that is, defending against, and responding to, cyber intrusions into U.S. systems and networks as well as the conduct of U.S. offensive cyber intrusions. While the DoD report did highlight many of the difficult issues in analyzing and applying the law of armed conflict to cyber operations and noted that there were risks to conducting them, it did not find any significant legal impediments to such operations.¹¹²

Much like the case of a state which finds itself the victim of a use of force, a state faced with an intrusion into its computer systems or networks would have to not only characterize the nature of the intrusion, but then formulate an appropriate, and lawful, response. In the least serious scenario,

[a]ny unauthorized intrusion into a nation’s computer systems would justify that nation at least in taking self-help actions to expel the intruder and to secure the system against reentry. An unauthorized electronic intrusion into another nation’s computer systems may very well end up being regarded as a violation of the victim’s sovereignty. It may even be regarded as equivalent to a physical trespass into a nation’s territory.¹¹³

In the more serious cases, a series of widespread, unauthorized, foreign intrusions from what appears to be the same source may

¹¹¹ *Id.* at 12.

¹¹² *Id.* at 50 (“There are no “show-stoppers” in international law for information operations as now contemplated in the Department of Defense”).

¹¹³ *Id.* at 19.

indicate both that there is a continuing danger and that coercive measures are necessary to stop the intruder's pattern of conduct. Similarly, there may be a right to use force in self-defense against a single foreign electronic attack in circumstances where significant damage is being done to the attacked system or the data stored in it, when the system is critical to national security or to essential national infrastructures, or when the intruder's conduct or the context of the activity clearly manifests a malicious intent. If it is capable of doing so, in such circumstances the victim nation may be justified in launching a computer attack in response . . . Either response would likely be analyzed on the basis of the traditional criteria of necessity and proportionality.¹¹⁴

Similarly, much like troops pursuing retreating forces in an armed conflict, a state that continues to face a threat from cyber attacks, although no longer ongoing, would not necessarily have to end its response.¹¹⁵

Ultimately it will be up to the victim state to determine whether such act was a use of force and, if so, what response it will take.¹¹⁶ This view is reflected in the DoD memo which stated: "[t]he issue for the victim is to choose the most effective available sanction. The issue for a nation contemplating an action that may be considered to violate the rights of another nation under international law is to accurately predict what sanctions such action may provoke."¹¹⁷ While this statement was meant to apply to acts of cyber intrusion, it applies equally as well to hostile acts which do not rise to the level of an armed attack and, outside of United Nations Security Council Resolutions addressing such incidents, remains largely the case.

While the approach of applying the law of armed conflict by analogy based on the consequences or effects of a cyber activity is the most commonly accepted one to date, other analytical frameworks have been proposed. Some have proposed an instrumentality approach. This analysis looks at whether the tool used to conduct the activity is a weapon; if so, its use would be considered a use of force. This approach is too narrow as it fails to consider the harmful effects that may be caused by cyber tools with multiple uses and has been fairly widely rejected.

¹¹⁴ *Id.* at 20.

¹¹⁵ DoD OGC Memo, *supra* note 67, at 23.

¹¹⁶ *Id.*

¹¹⁷ *Id.* at 17.

Another alternative analytical framework to the application of the traditional Article 2(4) *jus ad bellum* approach in regulating cyber attacks has been proposed by Professor Michael Schmitt.¹¹⁸ While this framework focuses on the consequences of the cyber activity, it expands on the previous approach that looked to the consequences of the actions in light of Article 2(4).¹¹⁹ Schmitt limits his analysis to the question of “[w]hen does a computer network attack conducted by, or on behalf of, a state constitute a wrongful use of force under international law.”¹²⁰ This focus detracts from the usefulness of the proposed framework as this mode of conflict is becoming anachronistic in the realm of cyber attacks. The anonymous capability of the Internet has become the standard technique when conducting cyber intrusions and makes it difficult if not impossible to determine whether those conducting the activity are doing so on behalf of a state.

Rather than developing a new system or standard to apply to cyber attack as a use of force, Schmitt proposes working within the current system to address the changing nature of the threat in light of cyber attack and cyber intrusion capabilities. He recognizes that the development of these cyber capabilities calls for the development of a new legal framework within which the new nature of cyber attacks may be considered, but also recognizes that the development of a new framework is not likely to occur in the short term.¹²¹ In order to deal with the new cyber capabilities, Schmitt proposes a method of analysis within the current U.N. Charter use of force structure.

Schmitt explains that, much like in the analysis of the use of force, some aspects of cyber attacks are more easily categorized than others. Cyber attacks that result in death, injury or physical destruction of property would be considered a use of force no different than had kinetic force been used to achieve the same results.¹²² As discussed previously, the law of armed conflict does not focus just on the instrumentality used, but rather looks at the results or consequences of the act.¹²³ This approach limits the analysis and characterization of a cyber attack to one that determines whether the cyber attack is a use of force or not.¹²⁴ If it is a use of force, then it is prohibited unless some authority to conduct that attack can be found within the Charter.¹²⁵ If it is not equivalent to a use of force, then it is permissible and not prohibited by Article 2(4).

¹¹⁸ Schmitt, *CNA*, *supra* note 10, at 886.

¹¹⁹ *Id.*

¹²⁰ *Id.* at 889.

¹²¹ *Id.* at 934.

¹²² *Id.* at 913.

¹²³ Schmitt, *CNA*, *supra* note 10, at 913.

¹²⁴ *Id.* at 901-902.

¹²⁵ *Id.* at 902.

Schmitt also recognizes that the line between prohibited use of force and coercive, but permissible, political and economic measures has been further blurred with the development of cyber attack and cyber intrusion capabilities.¹²⁶ The discussion, both during the drafting of the U.N. Charter and in other international fora, sheds some light on what measures were not to be considered as a use of force, but relatively little insight into what was intended to be covered, outside an armed attack, as a prohibited use of force. Although most would agree that the prohibition on the threat or use of force includes armed force and does not include political or economic coercion, what lies in between is mostly still shrouded in doubt.¹²⁷ This gray area created some problems before the development of cyber capabilities, but has been significantly expanded since.

This approach ignores whether it might be possible for a cyber attack or cyber intrusion to not a use of force or an armed attack, but yet have such consequences that the conduct of that activity and its consequences might be a “threat to the peace” and, therefore, within the jurisdiction of the U.N. Security Council for possible remedial action under Chapter VI or Chapter VII.

Schmitt argues that the current Chapter VII security framework is sufficient to handle the threat to international peace and security posed by cyber attack and cyber intrusion.¹²⁸ In explaining the Charter’s use of force structure, Schmitt states:

Thus, faced with CNA that does not occur in conjunction with, or as a prelude to, conventional military force, a state may only respond with force in self-defense if the CNA constituted armed force by the standard enunciated *supra* for armed force, i.e., that it is intended to directly cause physical destruction or injury. The victim state could repair to the Security Council and allege that other acts of CNA threaten the peace and merit a Chapter VII response, but it could not respond forcefully thereto on its own accord. Additionally, computer network attacks falling short of armed attack might nevertheless violate Article 2(4)’s prohibition on the use of force, thereby subjecting the actor to international opprobrium, but not to a response in self-defense.¹²⁹

¹²⁶ *Id.* at 907-908.

¹²⁷ *Id.* at 908.

¹²⁸ Schmitt, *CNA*, *supra* note 10, at 886.

¹²⁹ *Id.*

The DoD General Counsel Memo echoes this belief that the U.N. Charter's Chapter VII structure could be effective in dealing with cyber activity that falls short of an armed attack.¹³⁰

Nothing would prevent the Security Council from finding that a computer network attack was a "threat to the peace" if it determined that the situation warranted such action. It seems unlikely that the Security Council would take action based on an isolated case of state-sponsored computer intrusion producing little or no damage, but a computer network attack that caused widespread damage, economic disruption, and loss of life could well precipitate action by the Security Council.¹³¹

Schmitt's reliance on the Security Council and its Chapter VII authority in dealing with cyber threats is misplaced. When faced with a cyber threat to international peace and security, relying on Security Council action would be largely ineffective, as it would not occur in time given the immediacy with which cyber attacks occur and their effects are felt. Additionally, it is unlikely that the political divisions among the veto-wielding P-5 could be overcome. In addition to the usual political divisions, there is the fact that the U.S., Russia, and China are all "usual suspects" of coercive cyber activity and may very well be involved in the activity that is the subject of complaint.

Schmitt does point out that there have been recent developments where states have responded with their own use of force, outside of Charter provisions, to threats to community values, such as genocide and crimes against humanity, stating,

in many cases states have responded to situations, either individually or in concert, in which community interests were served by taking coercive measures not specifically provided for in the Charter. Such incidents combine to map out a complex operational code as to those coercive acts the international community, or at least the politically relevant members thereof, accepts as lawful.¹³²

The potential for disparity between a prohibited use of force and permissible economic coercion has been noticed before.¹³³ The effects of a limited armed attack, while causing immediate physical destruction, may be felt

¹³⁰ DoD OGC Memo, *supra* note 67, at 15.

¹³¹ *Id.*

¹³² Schmitt, *CNA*, *supra* note 10, at 902.

¹³³ *Id.* at 909.

for a much shorter period of time, and in a more restricted geographical area, than those created by coercive economic measures.¹³⁴

Schmitt argues:

Nevertheless, instrument-based evaluation is merited in the case of the former, but not the latter, by virtue of its far greater consequence-instrument congruence. Armed coercion usually results in some form of physical destruction or injury, whereas economic (or political) coercion seldom does. Additionally, the risk of an escalating conflict from a use of force ordinarily exceeds the risk from economic or political coercion because force strikes more directly at those community values at the top of the human hierarchy of need, in particular survival. The fact that the consequences of the use of force are almost immediately apparent, whereas economic or political consequences, although severe, emerge much more slowly, and thereby allow opportunity for reflection and resolution, compounds the danger of escalation.¹³⁵

Because force represents a consistently serious menace to intermediate and ultimate objectives, the prohibition of resort to it is a relatively reliable instrument-based surrogate for a ban on deleterious consequences. It eases the evaluative process by simply asking whether force has been used, rather than requiring a far more difficult assessment of the consequences that have resulted.¹³⁶

Schmitt further argues that linking cause and effect in cases of economic and political coercion is more difficult than in the case of armed force because of the “time lag” between the initiation of the coercive measures and the emergence of the consequences of those actions.¹³⁷ This problem also makes the application of the law of armed conflict to cyber attacks difficult. The time lapse between the initial cyber intrusion and the consequences resulting from those actions may be weeks, months, or even years. Compounding this gap between activity and consequence is the uncertainty as to the cause of the effects. Many other acts may intervene to alter the intended results, bringing about far greater consequences than intended.

¹³⁴ *Id.* at 909-910.

¹³⁵ *Id.* at 911-912.

¹³⁶ *Id.* at 911.

¹³⁷ Schmitt, *CNA*, *supra* note 10, at 912.

In the cyber realm, it is often likely that all of the possible consequences from an activity may not be ascertainable. The interconnectivity of the Internet makes the likelihood of unintended second- and third-order effects far greater than with the use of armed force, or even in the case of economic or political coercion. Exactly how an activity will be routed through the systems and networks of the Internet does not remain constant. The actions of others using those same systems and networks may unintentionally compound the effects of the intended action.

Schmitt goes on to explain:

Computer network attack challenges the prevailing paradigm, for its consequences cannot easily be placed in a particular area along the community values threat continuum. The dilemma lies in the fact that CNA spans the spectrum of consequentiality. Its effects freely range from mere inconvenience (e.g., shutting down an academic network temporarily) to physical destruction (e.g., as in creating a hammering phenomenon in oil pipelines so as to cause them to burst) to death (e.g., shutting down power to a hospital with no back-up generators). It can affect economic, social, mental, and physical well-being, either directly or indirectly, and its potential scope grows almost daily, being capable of targeting everything from individual persons or objects to entire societies.¹³⁸

Schmitt argues that international law regarding coercion is shorthand for trying to limit adverse consequences to international community values. Because it is difficult, if not impossible, to prohibit adverse consequences, the law of armed conflict attempts to limit the mechanisms that bring about those consequences. At the time of the drafting of the U.N. Charter, those adverse consequences and the dangers they posed to community values stemmed almost totally from the use of force. The focus of the use of force was to destroy the opponent's military capabilities by destroying either his military forces, his resources needed for those capabilities, or, in the case of aerial bombardment in WWII, the will of the people to support and fight. Modern warfare, while still largely focused on physical destruction, is beginning to move away from this twentieth-century paradigm and is becoming more "effects based." That is, military thinking is beginning to move away from the focus on tools/weapons and is moving towards thinking about consequences and how to achieve those which are desired. Whether this shift in thinking is developing because of new

¹³⁸ *Id.*

capabilities like cyber attack, or whether the benefits of such an approach themselves have caused it, can be debated.

Schmitt also argues that the right to use force in self-defense in response to a cyber attack be limited to those “operations which are de facto armed attacks, or imminently preparatory thereto.”¹³⁹

The overwhelming common interest in basic order, and the exorbitant potential costs of exercise of force by contemporary weapons would appear to counterbalance losses states may occasionally incur from lesser wrongs left inadequately redressed because of deficiencies in available remedial procedures or the limited ability of a poorly organized community to create effective remedies for all wrongs.¹⁴⁰

In the end, Schmitt argues for a continued restrictive approach when analyzing cyber attacks as a use of force.

[M]aintaining a relatively high threshold for triggering the right to respond to CNA in self-defense, although not enhancing its deterrent effect, serves to maintain constraints on the usually more disruptive act of unilateral resort to armed force. Furthermore, should an information operation be mounted that raises the question of whether an act of armed force has occurred, it would in all likelihood amount to a threat to the peace and thereby seize the Security Council of the matter. This may be faint consolation for the state facing a serious computer network attack, but from a world order perspective it represents the optimal alternative.¹⁴¹

Schmitt’s article was written in 1999. Since then the threat from cyber attack has continued to grow. Cyber intrusions have grown not only in number, but also in type. Schmitt’s argument that other states would soon challenge the U.S. for dominance in offensive cyber capabilities has already arrived. While many of the points made by Schmitt in his article are still valid, the vulnerabilities that existed then have only grown, as has the importance of the Internet and U.S. reliance on it.

¹³⁹ *Id.* at 886.

¹⁴⁰ *Id.* at 937.

¹⁴¹ *Id.* at 936-937.

V. THE CYBER THREAT AS A FUNDAMENTAL CHANGE IN THE NATURE OF WARFARE

*"[T]he categories of warfare are blurring and no longer fit into neat, tidy boxes. One can expect to see more tools and tactics of destruction – from the sophisticated to the simple – being employed simultaneously in hybrid and more complex forms of warfare."*¹⁴²

A. Cyber warfare as "hybrid" or "unrestricted" warfare

Cyber warfare has fundamentally changed the nature of conflict, expanding it both spatially and temporally, while also reducing potential death, injury and physical destruction. The growing importance of the Internet to a state's economic, diplomatic, and military interests has created a new arena in which states pursue these interests and compete with potential adversaries. The relative anonymity of cyber operations allows states to covertly pursue their own interests, and challenge the interests of adversaries, with a reduced risk of attribution and retribution. Perhaps most importantly, the growing interconnectedness of government information systems has created the opportunity for adversaries to engage in aggressive cyber espionage, collecting more information than could have otherwise been obtained via traditional espionage techniques.¹⁴³ Combined, these attributes present an opportunity for weaker states to gain an asymmetrical advantage over traditional military powers by engaging in cyber warfare.

Thus, cyber warfare should not be viewed in the limited scope of physical destruction of hardware, software or information resident on networks but must be viewed in a much broader scope. Manipulating information in order to influence public opinion, disrupting services to reduce confidence in systems, and gaining access to systems are all activities that take place thousands of times each day and are directed against U.S. governmental and private systems and networks. All of these activities fall below the use of force. While the law of armed conflict applies to those activities which do reach the level of a use of force, that portion of activities covered is actually quite small.

Further, a state may engage in this type of conflict on a broader scale, both temporally and spatially, as almost all such activity would fall below the threshold of a use of force. The rise of the Internet and its importance has created an entirely new sphere of conflict. Operations in this area are being conducted not only in preparation for an armed conflict, should one break out,

¹⁴² Robert M. Gates, *A Balanced Strategy*, FOREIGN AFFAIRS, Jan.-Feb. 2009, <http://www.foreignaffairs.com/articles/63717/robert-m-gates/a-balanced-strategy>.

¹⁴³ Brenner remarks, *supra* note 23.

but have also taken on their own importance and are seen as an area where a state may advance its own interests against competitors without risking open conflict.

The Internet has emerged as a key component of the U.S. and global economy. The Internet has also brought about a seismic shift in how we think about information. With the increasing reliance of economic, social, governmental, and defense activities on the Internet, the truism “information is power” has taken on an entirely new meaning. The very element that makes the Internet such a valuable resource is also its greatest weakness, its interconnectedness.¹⁴⁴ Additionally, this feature also makes predicting, or limiting, the consequences of a cyber attack problematic.¹⁴⁵ While in the past states involved in a conflict may have been able to affect an opponent’s information and use of information at the margins through deception, propaganda, and espionage, the capability now exists to conduct such operations on a much broader and more intense scale because of U.S. reliance on the Internet.

Although the nature of warfare has been and will continue to be changed, certain elements will have familiar characteristics. Rather than risk an open, widespread, conflict that would result in large-scale destruction and death, or even a widespread cyber war that would devastate the global economy, states may choose to engage in conflict through surrogates and proxies in cyber space. Continuous, low-level conflict in cyber space marked by frequent and widespread espionage activities and sporadic and low-scale attacks may represent the next Cold War, but one engaged in by three main powers.

Domestic criminal law also offers little in the way of a deterrent because many of the most dangerous acts are committed by state actors and are actually conducted outside the U.S. It is important that those developing this new strategy understand the lacunae in the legal regimes applicable to cyber activities. The problems include the difficulty in attributing the acts to a particular actor, as well as determining the purpose of the acts. If the victim is assured that the intrusion is only to gain information, the response may be quite different than if the victim believes that the intrusion is really the first step in laying malicious code that will be used to bring about some destructive effects.

Although many states have developed capabilities to engage in cyber espionage and cyber attacks, perhaps none have done as much to further their cyber capabilities as China. China has focused on developing both the technical and personnel capabilities needed to engage in an extended cyber conflict. In

¹⁴⁴ Schmitt, *CNA*, *supra* note 10, at 893.

¹⁴⁵ *Id.*

recent testimony before the U.S. China Economic and Security Review Commission, it was announced that China has developed and begun installing a secure operating system on government systems.¹⁴⁶ This system, known as Kylin, makes it much more difficult for the U.S. to engage in offensive cyber operations against Chinese systems on which it is installed, and may give a significant advantage during any cyber conflict.¹⁴⁷ It was also reported that the Chinese have developed a secure microprocessor that will further improve Chinese cyber defenses against U.S. intrusions.¹⁴⁸ The expert discussing these developments remarked “that in the cyberarena, China is playing chess while we’re playing checkers.”¹⁴⁹

China is also developing personnel with the expertise to conduct cyber intrusions and attacks. In recent testimony before the Senate Committee on Homeland Security and Governmental Affairs, Allan Paller reported on Chinese graduate student Tan Dailin.¹⁵⁰ After winning a hacking competition, the Chinese military sent Tan to a 30-day, 16-hour-a-day course to further develop his hacking skills.¹⁵¹ Tan then competed in, and won, several other cyber contests against Chinese military units before establishing a company in September 2005.¹⁵² In December 2005 Tan’s company was detected penetrating DoD computers.¹⁵³

In addition to developing advanced cyber capabilities that could be used to conduct espionage and attacks targeting the U.S., China has developed a comprehensive cyber strategy that reflects the strategic importance of the Internet and cyber operations. Chinese information warfare theory has long been based on the concept that warfare is constant, that it is ongoing, and that efforts must be made now, in times before the outbreak of physical violence, to lay the groundwork for success in the physical domain.¹⁵⁴

The asymmetric advantage offered by cyber warfare has the potential to negate much of the United States’ conventional military strength. Rather than relying solely on traditional naval power to advance its security interests, China is investing heavily in cyber warfare capabilities which could seriously threaten

¹⁴⁶ Bill Gertz, *China Blocks US from Cyber Warfare*, WASHINGTON TIMES, May 12, 2009, available at <http://washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/print/>.

¹⁴⁷ *Id.*

¹⁴⁸ *Id.*

¹⁴⁹ *Id.*

¹⁵⁰ *Id.*

¹⁵¹ Gertz, *supra* note 146.

¹⁵² *Id.*

¹⁵³ *Id.*

¹⁵⁴ Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies (Dec. 2007), available at http://www.potomac institute.org/publications/Potomac_HybridWar_0108.pdf.

U.S. ability to project power and defend allies in the western Pacific.¹⁵⁵ Other states will also seek to capitalize on the asymmetric advantage offered by cyber activities, a fact that the United States must now deal with by not only developing a strategy for this shift in the nature of warfare but also recognizing the effect it has on the existing law of armed conflict paradigms.

When viewed in the context of the law of armed conflict paradigm, the use of the terms “cyber warfare” and “cyber attack” to refer to this malicious cyber activity adds confusion to an already difficult topic. If, however, this activity is analyzed in the context of the threat posed to U.S. national security, these terms may more accurately reflect the situation in which the U.S. finds itself. In fact, the development of cyber intrusion, exploitation, and attack capabilities, and the methods in which they are being used against the U.S., have changed the very nature of warfare, and U.S. national security strategy, the paradigms upon which that strategy was formed, and the legal regimes that frame that strategy must be revised to reflect this change.

B. The Challenge of Attribution

“One major implication is that it may be very difficult to attribute a particular computer network attack to a foreign state, and to characterize its intent and motive.”¹⁵⁶

Cyber attacks are not accompanied by calling cards. Perhaps the single greatest challenge to the application of the law of armed conflict to cyber activity is the challenge of attribution.¹⁵⁷ Outside of traditional state-on-state armed conflicts, states targeted by cyber attacks will likely not be able to determine, with any certainty, who is responsible for the attack.¹⁵⁸ While it may be possible, given the right technological capabilities or inferring from the target and nature of the activity, to narrow down the field of suspects, it is also possible for a technologically sophisticated adversary to mask his activity as coming from a third source.

The difficulty in attributing the source of a cyber attack or cyber intrusion presents several legal challenges. First, in those cases where the response will not rise to the level of being a use of force, any action taken against the apparent source of the attack without the consent of the state where it

¹⁵⁵ Gates, *supra* note 142.

¹⁵⁶ DoD OGC Memo, *supra* note 67.

¹⁵⁷ “It is nearly impossible to know whether or not an attack is government-sponsored because of the difficulty in tracking true identities in cyberspace.” Gorban, *Electricity Grid Penetrated by Spies*, *supra* note 56.

¹⁵⁸ NRC Report, *supra* note 5, at 2.4.2.

is located or where the effect will be realized, would be a violation of that state's sovereignty. Second, a response that does rise to the level of a use of force must comply with the law of armed conflict principles of military necessity, distinction, proportionality, perfidy and neutrality.¹⁵⁹ A response against a civilian target that is not involved in the cyber attack would violate the principle of military necessity and distinction.

The ability to identify, and attribute, the source of a cyber attack or cyber intrusion has important political implications as well. As discussed above, malicious cyber activity that does not rise to the level of a use of force may still present a threat to international peace and security. A state that finds itself a victim of this type of activity would not be authorized to respond with force, but may desire to seek assistance from the U.N. Security Council. States may also want to garner international support, either defensive support or support to implement economic or diplomatic measures against the offending state. The victim state may wish to only shame the offending state, branding it in the eyes of the international community as a violator of international law or custom. Without some semblance of proof, the requested international support will likely never occur. Finally, while these acts are violations of domestic criminal law, the issue of attribution also makes prosecution, let alone identification, of the perpetrator highly unlikely.

It is unlikely that "absolute" attribution, or even attribution "beyond a reasonable doubt," will ever be achieved. However, efforts must be made to achieve attribution sufficient to meet law of armed conflict targeting requirements and to garner support in the court of public opinion. Solving the problem of attribution will require both improved technical capabilities as well as better intelligence.¹⁶⁰

C. Signaling Intent and Escalation

An issue related to the problem of attribution is the difficulty in determining the intent of the actor or the purpose of the activity. In many cases, the cyber attack may only be discovered once the effects of the attack become apparent. In other cases, an intrusion may be discovered before any effects have been identified. From the intended victim's viewpoint in these cases, it will be difficult, if not impossible, to determine whether the activity is being conducted to identify and gain access to the system or is being conducted to conduct

¹⁵⁹ Of course, a cyber response that would be considered a use of force would only be permissible if done in self-defense to an armed attack or pursuant to a United Nations Security Council Resolution and Chapter VII of the U.N. Charter.

¹⁶⁰ NRC Report, *supra* note 5, at 2.4.2.

computer espionage, in preparation for a later computer attack, to commit a purely criminal act, or merely as an act of vandalism.¹⁶¹

The difficulty in determining the intent of the actor creates a challenge for states in determining whether they would be permitted to use force to defend themselves from the cyber attack. A state may use force in self-defense preemptively in the face of an imminent attack. If, however, a state cannot determine whether the cyber attack is the first step of an imminent attack or whether it is merely a criminal act, it would be prohibited from using force in self-defense to counter the cyber attack. It would appear that, absent some other evidence of intent, a state would have to wait until the effects of the cyber attack are realized before responding with force to an intrusion into its systems or networks.

The problem then is one of signaling intent. Without being able to attribute the source of the act, the victim is not able to accurately judge the purpose, or intent, behind the act. For example, knowing that the act was perpetrated by a certain state, that is known to have certain capabilities, and whose general hostility towards the victim may be, may allow the victim to determine whether it is at a greater danger of risk of a more destructive attack. The problem is also tied to the problem that the initial intrusion which may be detected, and even perhaps the malicious code uncovered, may all appear very similar. It may be almost impossible to determine the purpose of the code until its effects have been realized. This gap between the initial act and the manifestation of its consequences carries with it a danger of escalation.¹⁶²

The similarity in characteristics between acts conducted in preparation for a future cyber attack and those conducted to gather intelligence further complicates efforts to defend against, and respond, to these acts.¹⁶³ The application of the law of armed conflict to this continuous, low-level, malicious cyber activity places states in a very difficult position. A state discovering these intrusions would find it difficult to determine not only the identity but also the intent of the perpetrator, and would apparently be prohibited from using force in self-defense until the consequences of the acts manifested themselves as an equivalent to that of an armed attack. These same characteristics also present a challenge for states conducting offensive cyber operations. Absent a mechanism by which intent is signaled, these operations carry a risk that the targeted state will respond to the intrusion with force, possibly even striking back at the wrong party and escalating hostilities.¹⁶⁴

¹⁶¹ *Id.* at 2.4.1.

¹⁶² *Id.*

¹⁶³ *Id.* at 1-3.

¹⁶⁴ *Id.* at 2.4.1.

VI. SUGGESTIONS FOR A WAY AHEAD

It is often said that the United States has more to lose from cyber attacks than any other state. It is true that the United States economy has become increasingly dependent on and connected to the Internet. This interconnectivity does not stop at the nation's borders. Any attack that disrupts the U.S. economy would have devastating effects on the global community.

This is especially true in the case of China. While China may be engaged in extensive cyber espionage against the United States, its own economy would suffer greatly from any attack that would disrupt U.S. commercial interests in cyber space. This weakness presented by the interconnected nature of the Internet and global economy may also offer the best opportunity for countering the threat. In fact, the way to counter the threat may be to increase the interconnectedness of the global economy. If other states realized that the effects flowing from an attack against the United States would not be contained within the borders of the U.S., but rather would spill over and affect their own vital economic interests, they would have greater incentive to police the electrons passing through their networks and systems.

In essence, one approach would be to remove the free-rider problem as much as possible by transferring the costs of policing cyber space, and the costs of any failure to adequately do so, to those in the best position to counter the threat. One method that could be used to accomplish could be a kind of cyber "Monroe Doctrine" whereby the United States declares that it will actively defend its interests in cyber space by engaging threats from wherever they emanate.¹⁶⁵ Knowing that a threat coming from or through their systems and networks, even if only transiting, will invoke a response may spur other states to take a more active role in the defense and policing of their networks. Another approach might be to develop some sort of international agreement similar to the Proliferation Security Initiative whereby states agree to work together to prevent cyber attacks emanating from, or passing through, their territories, networks and systems.

In proposing a strategy to deal with the threat posed by cyber intrusions and cyber attacks it is important to not try to achieve the impossible. Cyber exploitation - that is, cyber intrusions conducted to conduct espionage - are a low-risk, high-gain activity. There is very little risk of being caught and, even if

¹⁶⁵ See Hearing before the House Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, Statement of Mary Add Davidson, Chief Security Officer, Oracle, *available at* <http://homeland.house.gov/SiteDocuments/20090310143850-78976.pdf>.

caught while conducting the activity, there is very little risk that the activity will be attributed to the state conducting the activity.

The United States also has much to gain from conducting cyber espionage and would risk losing access to vast amounts of information if it was somehow prevented from conducting this activity. In fact, some scholars have even argued that less regulation of intelligence activities is actually better as it reduces the risk of sending mixed signals and allows adversaries to better read each others' intent.¹⁶⁶ Thus, any kind of international treaty that would purport to prohibit cyber espionage would certainly fail and may actually create more conflict. Additionally, entering into such an agreement and then failing to abide by it would damage the reputation of the United States.

A better approach would be to focus on measures that may be taken to limit destructive attacks, that is, cyber activities that would rise to the level of an armed attack and that would result in the greatest harm to U.S. national security. Focusing on this part of the problem alone would help focus on a more manageable problem set.

In some aspects, the development of a cyber strategy to deal with this new threat might mirror that of the development of the new counter-insurgency strategy. Such a strategy would recognize that military force alone is insufficient to counter the threat and that economic, diplomatic, and social aspects of cyber engagement must also be considered. Just as the doctrine and policies that were developed for the Cold War proved inadequate in countering insurgencies in Iraq, Afghanistan, and in the broader contest against violent extremism, they are also proving inadequate to carry this contest into cyber space.

The traditional break-down between the Departments of Defense, Justice, and State does not function well in cyber space. Countering one threat may require responses from several government agencies. Not only is there a "merging of previously discrete forms of war," there is also a merging of conflict with other activities in cyber space.¹⁶⁷ The U.S. government and DoD in particular must "learn how to fight efficiently across the spectrum of conflict."¹⁶⁸ Just as the military must be prepared to fight across the spectrum and deal with traditional conflicts, non-state, and trans-state threats, the United

¹⁶⁶ See Glenn Sulmasy and John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625 (2007).

¹⁶⁷ Michael Evans, *From Kandesh to Kandahar: Military Theory and the Future of War*, NAVAL WAR COLLEGE REVIEW, Summer 2003, at 139.

¹⁶⁸ *Id.*

States government as a whole must be prepared to act across the cyber spectrum, conducting espionage, diplomacy, covert action, and the use of force.

Similarly, the United States government as well as those private organizations that operate elements of critical infrastructure and resources must be able to recognize and react to the same actions by adversaries – both state and non-state adversaries. This will include recognizing what policy and legal limitations apply to both governmental actions and reactions as well as the actions and reactions of private organizations.

VII. CONCLUSION

The majority of cyber attacks conducted today do not rise to the level of an armed attack or a use of force. There is a general agreement that for a cyber attack to be considered as an armed attack, the consequences of the cyber activity must be equivalent to those of a kinetic attack, that is, the activity must cause physical damage, injury or death. Such an attack would justify the use of armed force by the victim in self-defense, with the accompanying duty to abide by LOAC in the use of that force. A state that found itself the victim of a cyber attack equivalent to a use of force, but not an armed attack, would be prohibited from using force to defend itself, but might take diplomatic or economic measures in response to the activity.

It is difficult, and in some cases impossible, to attribute these acts to a specific individual, organization or state, or even to a specific geographic location. It is assumed that these acts are conducted by a wide variety of actors, including individuals, criminal organizations, non-state actors (both for their own purposes as well as on behalf of a state), and official state actors. Most of these acts are conducted to gain access to information for some other purpose: state sponsored espionage, corporate espionage, or criminal activity such as identity theft and other financial crimes. Even those acts which are conducted to disrupt or damage information resident on systems and networks usually do not rise to the level of a use of force. Other acts are intrusions conducted in order to gain access for a future, perhaps more disruptive act, such as a computer network attack on critical infrastructures and systems.

The problem with this approach is that it fails to take into consideration the potential for cumulative damage caused by a series of lower-level cyber attacks. Manipulation of financial data, while not actually causing any physical damage, could result in an economic catastrophe of far greater consequences than would result from the destruction of physical infrastructure. Cyber espionage might cause much greater damage to the national security of the U.S. than the physical destruction of a weapons system or military facility. The

application of traditional *jus ad bellum* and *jus in bello* principles can be seen as creating an incentive for parties to engage in cyberwarfare by reducing the potential risk of retribution. Thus, limiting cyber attack responses to diplomatic or economic measures may not act as a sufficient deterrent to such activity. However, expanding allowable responses to include cyber attacks, or other acts, that rise to the level of a use of force, has the potential to escalate the situation into a broader, more violent conflict.

The development of cyber warfare requires a change in U.S. national security and defense strategy. As can be seen by the daily, continuous cyber attacks against critical infrastructure, systems and networks, potential adversaries have realized the strategic, asymmetrical advantage that can be gained over the U.S. by engaging in cyber warfare. This concept of unrestricted warfare recognizes that, through cyber warfare, a strategic advantage may be gained without ever having to resort to physical armed force. Rather than being limited in time and geographical location, cyber warfare is ongoing across both governmental and private networks and systems. The continued application of a law of armed conflict paradigm to modern conflict, one which is fundamentally different from that by which it was formed, will not only fail to protect the national security of the United States, but will also fail to protect the very interests it was designed to protect.

UNITED STATES ENVIRONMENTAL LAW APPLIED IN THE ARCTIC OCEAN: FRUSTRATING THE BALANCE OF THE LAW OF THE SEA, NATIONAL SOVEREIGNTY, AND INTERNATIONAL COLLABORATION EFFORTS

Lieutenant Commander Joan M. Malik¹

I. INTRODUCTION

Climate change evidence brings images of polar bears and their once ice-covered ocean spaces of the Polar Regions to the forefront of the minds of people throughout the world. Dire concern of opened polar oceans free of ice by as early as 2013, with commentary of faster-melting ice than once predicted, flies across the newswire every day.² U.S. government officials recognize both the need to engage with other Arctic nation-states³ and the need to set a national Arctic policy.⁴ Strategic, national security, economic and environmental protection reasons exist to do both.⁵ While the U.S. government postures about

¹ LCDR Joan M. Malik, JAGC, USN (LL.M. (*cum laude*) in Environmental and Natural Resource Law, 2009, Northwestern School of Law at Lewis & Clark College; J.D. (*cum laude*), 2000, New England School of Law; B.A. (*cum laude*), 1997, Loyola College in Maryland) is currently on active duty serving as Region Environmental Counsel for Commander, Navy Region Northwest in Silverdale, Washington. Invaluable insight and assistance were greatly appreciated from: Environmental faculty and classmates at Lewis and Clark Law School, Captain Jeffrey Luster, JAGC, USN, Captain Dean Leech, JAGC, USN and Commander Pam Ellen Hudson, USN (Ret'd). The author's views and opinions do not necessarily represent the views of the U.S. Navy, Department of Defense, or any other U.S. governmental agency.

² See Scott Borgerson, New U.S. Arctic Policy Gets It Mostly Right, Jan. 13, 2009, <http://securitydebrief.adfero.com/index.php/2009/01/13/new-us-arctic-policy-gets-it-mostly-right/>. As the Intergovernmental Panel on Climate Change predicts, "[t]he polar ice cap is melting fast, losing up to half its thickness near the North Pole in just the past six years and perhaps is passing a tipping point; it is now shrinking at more than three times the rate predicted by the IPCC only four years ago." *Id.*

³ These nations include Russia, Norway, Canada, Finland, Iceland, Denmark (Greenland), and Sweden.

⁴ See Directive on Arctic Region Policy, 1 PUB. PAPERS 47 (Jan. 9, 2009); see also Hillary Rodham Clinton, Secretary of State, Remarks at The Joint Session of the Antarctic Treaty Consultative Meeting and the Arctic Council, 50th Anniversary of the Antarctic Treaty (Apr. 6, 2009), <http://www.state.gov/secretary/rm/2009a/04/121314.htm>.

⁵ Clinton, *supra* note 4:

ratifying the United Nations Convention on the Law of the Sea (“UNCLOS”),⁶ other Arctic states have already laid claim to particular continental shelf boundaries through their submissions to the Commission on the Limits of the Continental Shelf per Article 76 of the UNCLOS.⁷ Separate from the

The warming of the Arctic has profound implications for global commerce, with the opening of new shipping routes. It raises the possibility of new energy exploration, which will, of course, have additional impacts on our environment. And Arctic warming has already [had] serious consequences for the indigenous communities that have made their homes there for many generations. The changes underway in the Arctic will have long-term impacts on our economic future, our energy future, and indeed, again, the future of our planet. So it is crucial that we work together. Here in Washington, the State Department coordinates Arctic policy for the United States, and I am committed to maintaining a high level of engagement with our partners on this. That starts with the Law of the Sea Convention, which President Obama and I are committed to ratifying, to give the United States and our partners the clarity we need to work together smoothly and effectively in the Arctic region. There are also steps we must take to protect the environment. For example, we know that short-lived carbon forcers like methane, black carbon, and tropospheric ozone contribute[] significantly to the warming of the Arctic. And because they are short lived, they also give us an opportunity to make rapid progress if we work to limit them. In advance of the Arctic Council meeting in Norway later this month, I have asked my team here at the State Department to come up with new initiatives that the United States will put forth to be a full, active partner in these efforts.

⁶ United Nations Convention on the Law of the Sea, Dec. 10, 1982, 21 I.L.M. 1261, *available at* http://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm [hereinafter UNCLOS]. The United States has not ratified the treaty but since 1983, it has “abid[ed] by, and enjoy[ed] the rights accorded by, the provisions of the Convention covering the traditional uses of the ocean in accordance with the Ocean Policy Statement issued by President Ronald Reagan.” U.S. Department of State, “Law of the Sea Convention,” *available at* <http://www.state.gov/g/oes/ocns/opa/convention/index.htm> (last visited Mar. 9, 2010). Many federal agencies support ratification of the Convention. *See id.*; *see also* Testimony of Rear Admiral Arthur E. Brooks, Commander, Seventeenth Coast Guard District, U.S. Coast Guard before Alaska House State of Affairs Committee (Mar. 2009) *available at* <http://www.uscg.mil/comdt/blog/2009/03/un-convention-on-law-of-sea-treaty.asp> (noting that UNCLOS balances the exclusive interests of coastal states in controlling activities off their coasts against the inclusive interest of all States in freedom of navigation and overflight). Given climate change and the changing operating environment for military that may allow more ice-free access in the maritime environment of the Arctic, the Department of Defense supports cooperative engagement in the Arctic and ratification of UNCLOS. *See* Department of Defense, Quadrennial Defense Review Report 86 (Feb. 2010), *available at* <http://www.defense.gov/QDR/>.

⁷ *See* Commission on the Limits of the Continental Shelf, Receipt of the Submission made by the Russian Federation, UN Doc. CLCS.01.2001.LOS (Continental Shelf Notification) (2001), *available at* http://www.un.org/Depts/los/clcs_new/commission_submissions.htm; Commission on the Limits of the Continental Shelf, Information About the Submission by Norway (2006), *available at* http://www.un.org/Depts/los/clcs_new/submissions_files/submission_nor.htm; *see also* U.S. Department of State, Bureau of Oceans and International Environmental and Scientific Affairs, Extended Continental Fact Sheet (Mar. 9, 2009), *available at* <http://www.state.gov/g/oes/rls/fs/2009/120185.htm>. In April 2009, three years after its initial submission, Norway

progressing boundary-settling since UNCLOS's entry into force in 1994, the Arctic's legal regime consists of a mix of international "soft law,"⁸ national domestic law of individual Arctic nations, and policy and "coordinated activities of the Arctic Council and its Working Groups."⁹ UNCLOS provides the key integral framework convention for the oceans that serves to assist the Arctic nations not just to delineate their sovereign boundaries but also to "present[] a general package of principles for possible regulations and treaties on marine environmental protection."¹⁰ From the perspective of a U.S. federal agency involved in activities within the Arctic ocean, there are several areas of concern: the currently shifting claims under UNCLOS; the extent domestic environmental laws may be applicable to the Arctic ocean; and whether those federal laws, particularly the National Environmental Policy Act ("NEPA"),¹¹ Endangered Species Act ("ESA")¹² and the Marine Mammal Protection Act ("MMPA")¹³ should apply extraterritorially. Therefore, this article will explain first why such issues are of importance to the United States, and then the activities that U.S. agencies conduct within the Arctic and how the domestic laws have been interpreted by U.S. courts to apply within the various maritime zones. Ultimately this article concludes that, given the Arctic's unique cooperative governance scheme, federal agencies should tread lightly in extending application of U.S. laws to the Arctic Ocean.

Contrary to what some may desire, no single "Arctic" multi-national treaty exists such as the one developed for Antarctica, nor is there a "[n]orthern movement to replicate the 'nature reserve' of the South Pole."¹⁴ But many legal

received a positive recommendation from the U.N. Commission for the Limits of the Continental Shelf regarding its claim to the extended continental shelf in the Norwegian Sea, the Barents Sea and the Arctic Ocean. See U.N. Backs Norway Claim to Arctic Seabed Extension (Apr. 15, 2009), <http://www.continentalshelf.org/news.aspx>. For a clear summary of claims of Russia and Norway, see Vladimir Jares, *The Continental Shelf beyond 200 M, the Work of the Commission on the Limits of the Continental Shelf, and the Arctic*, 42 VAND. J. TRANSNAT'L. L. 1265 (2009).

⁸ In international law parlance, the term refers to guidelines, codes of practice or standards from an "instrument that has no strict legal value but constitutes an important statement." Encyclopedia Britannica, available at <http://www.britannica.com/EBchecked/topic/930536/soft-law> (last visited Mar. 9, 2010).

⁹ LINDA NOWLAN, ARCTIC LEGAL REGIME FOR ENVIRONMENTAL PROTECTION x (2001).

¹⁰ Hans H. Hertell, Note, *Arctic Melt: The Tipping Point for an Arctic Treaty*, 21 GEO. INT'L ENVTL. L. REV. 565, 574 (2009) (quoting Thomas Hofer & Lutz Mez, *Effectiveness of International Environmental Protection Treaties on the Sea Transport of Mineral Oil and Proposals for Policy Revision*, in INTERNATIONAL MARINE ENVIRONMENTAL LAW 101, 103 (Andree Kirchner ed., 2002)).

¹¹ National Environmental Policy Act of 1969, 42 U.S.C.A. § 4321 *et seq.* (West 2009).

¹² Marine Mammal Protection Act of 1972, 6 U.S.C.A. § 1361 *et seq.*, 1401-1407, 1538, 4107 (West 2009).

¹³ Endangered Species Act of 1973, 16 U.S.C.A. § 1531-1544 (as amended) (West 2009).

¹⁴ NOWLAN, *supra* note 9, at x.

scholars debate whether an eventual Arctic-specific treaty will emerge.¹⁵ Rather than an all-encompassing treaty of obligations in the Arctic, the eight Arctic nations rely on cooperative initiatives, such as the Arctic Environmental Protection Strategy (“AEPS”) signed by the eight nations in 1991 to deal with just environmental protection.¹⁶ Other multilateral arrangements between the Arctic states have concerned marine mammals, scientific cooperation and defense of North America.¹⁷ The Arctic Council, an international high-level forum established in 1996 as an outgrowth of the AEPS, handles issues of sustainable development in addition to environmental protection. The Arctic Council is not a legally binding authority on the Arctic states, but it holds ministerial meetings every two years with decision-making occurring by consensus. The participants include Arctic states as well as “permanent participants that represent indigenous nations of the Arctic.”¹⁸ The Arctic Council’s objective is to “promot[e] co-operation, co-ordination, and interaction

¹⁵ See Tavis Potts & Clive Schofield, *An Arctic Scramble? Opportunities and Threats in the (Formerly) Frozen North*, 23 INT’L J. OF MARINE & COASTAL L. 151 (2008) (identifying three potential scenarios for Arctic governance in the future); Barry Hart Dubner, *On the Basis for Creation of a New Method of Defining International Jurisdiction in the Arctic Ocean*, 13 MO. ENV’T L. & POL’Y REV. 1 (2005) (advocating the establishment of an international boundary line that equates to an international park in the Arctic Ocean); Erika Lennon, *Environmental Change in Polar Regions: A Tale of Two Poles: A Comparative Look at the Legal Regimes in the Arctic and the Antarctic*, 8 SUSTAINABLE DEV. L. & POL’Y 32 (2008) (suggesting now is the time to create binding law in the Arctic that is similar to the Antarctica Treaty System to protect the environment); Hertell, *supra* note 10, at 574; Stephanie Holmes, Comment, *Breaking the Ice: Emerging Legal Issues in Arctic Sovereignty*, 9 CHI. J. INT’L L. 323 (2008) (suggesting the Antarctica Treaty System as a “loose” model for a treaty in the Arctic).

¹⁶ Hertell, *supra* note 10, at 574, 576.

¹⁷ With respect to marine mammals, Greenland, Norway, Iceland and the Faroe Islands signed the “Agreement on Cooperation in Research, Conservation and Management of Marine Mammals in the North Atlantic,” on April 9, 1992 and formed The North Atlantic Marine Mammal Commission. See The North Atlantic Marine Mammal Commission, “Agreement on Cooperation in Research, Conservation, and Management of Marine Mammals in the North Atlantic,” available at http://www.nammco.no/Nammco/Mainpage/DocumentsAndInformation/nammco_agreement.html (last visited Mar. 10, 2010). The Commission “provides a mechanism for cooperation and conservation on management for all species of cetaceans...and pinnipeds...in the region, many of which have not been covered by an international agreement.” The North Atlantic Marine Mammal Commission, available at <http://www.nammco.no/> (last visited Mar. 10, 2010). Fourteen nations currently take part in the International Arctic Science Committee (“IASC”), a non-governmental scientific organization that facilitates international cooperation and coordination in Arctic research. See Polar Research Board, available at <http://dels.nas.edu/prb/iasc.shtml> (last visited Mar. 10, 2010). Members of the IASC Council are selected by appropriate scientific committees in the participating countries. See *id.* The Polar Research Board, a unit of the National Academies, serves as the U.S. National Committee to IASC. See *id.* Canada and the United States established an arrangement for defense of North America by creating the North American Air Defense Command (“NORAD”) in 1958. See Natalie Mychajlyszyn, “The Arctic: Geopolitical Issues” 4 (Oct. 24, 2008) available at <http://www2.parl.gc.ca/content/lop/researchpublications/prb0806-e.htm>.

¹⁸ Potts & Schofield, *supra* note 15.

among the Arctic states, with the involvement of the Arctic indigenous communities and other Arctic inhabitants on common arctic issues, but [it is limited from dealing] with matters related to military security.”¹⁹ The Council created working groups that address various scientific, environmental and social issues.²⁰ Various non-Arctic-specific treaties provide a legal framework for safety of navigation and prevention of marine pollution, ocean dumping, and air pollution.²¹ The International Maritime Organization (“IMO”) and Arctic Council created guidelines on ship operations in the Arctic, Arctic offshore oil and gas activities, and environmental impact assessment in the Arctic.²² Given this framework for governance, on April 29, 2009, the Arctic nations reaffirmed in the Tromsø Declaration a commitment to cooperate among themselves toward “promoting environmental protection and sustainable use of Arctic Land and marine resources,” and they identified the pressing issues and guidelines for the Arctic Council’s work for the next two years.²³

¹⁹ NOWLAN, *supra* note 9, at 9.

²⁰ For information on the six working groups of the Arctic Council, *see generally* The Arctic Council, Working Groups, http://arctic-council.org/section/working_groups (last visited Sept. 27, 2009).

²¹ *See generally* International Convention for the Safety of Life at Sea, Nov. 1, 1974, 32 U.S.T. 47, 1226 U.N.T.S. 213 (as amended), *available at* <http://www.austlii.edu.au/au/other/dfat/treaties/1983/22.html>; International Convention for the Prevention of Pollution by Ships, Nov. 2, 1973, 12 I.L.M. 1319 (1973), *as amended by* Protocol of 1978 Relating to the International Convention for the Prevention of Pollution from Ships, Feb. 16, 1978, 17 I.L.M. 546 (1978), *available at* <http://www.austlii.edu.au/au/other/dfat/treaties/1988/29.html>; Convention on the Prevention of Marine Pollution by Dumping Wastes and Other Matter, Dec. 29, 1972, 26 U.S.T. 2403, 1046 U.N.T.S. 120, *available at* <http://www.admiraltylawguide.com/conven/dumping1972.html>; Protocol to the 1972 Convention on the Prevention of Marine Pollution by Dumping Wastes and Other Matter, Nov. 8, 1996, 36 I.L.M. 1, *available at* <http://www.admiraltylawguide.com/conven/protodumping1996.html>; Montreal Protocol on Substances that Deplete the Ozone Layer, Sept. 15, 1987, S. Treaty Doc. No. 100-10, 1522 U.N.T.S. 3 (as amended) (with Annexes) (entered into force Jan. 1, 1989), *available at* <http://www.unep.org/OZONE/pdfs/Montreal-Protocol2000.pdf>; United Nations Framework Convention on Climate Change, May 9, 1992, S. Treaty Doc. No. 102-38, 1771 U.N.T.S. 107 (with Annexes) (entered into force Mar. 21, 1994), *available at* <http://unfccc.int/resource/docs/convkp/conveng.pdf>;

²² *See generally* International Maritime Organization, Guidelines for Ships Operating in Arctic Ice-Covered Waters, IMO Doc. MSC/Circ. 1056 MEPC/Cir. 399 (Dec. 23, 2002), *available at* http://www.imo.org/includes/blastDataOnly.asp/data_id%3D6629/1056-MEPC-Circ399.pdf; Arctic Council, Protection of the Arctic Marine Environment Working Group, Arctic Offshore Oil & Gas Guidelines (Apr. 29, 2009), *available at* <http://arctic-council.org/filearchive/Arctic%20Offshore%20Oil%20and%20Gas%20Guidelines%202009.pdf>; Arctic Environmental Protection Strategy, Guidelines for Environmental Impact Assessment (EIA) in the Arctic (1997), *available at* <http://arcticcentre.ulapland.fi/aria/index.asp>.

²³ Arctic Council, Tromsø Declaration (Apr. 29, 2009), *available at* <http://arctic-council.org/filearchive/Tromsø%20Declaration-1..pdf>. Given this commitment to the Arctic Council framework, the United States is not pressing for a “new comprehensive Arctic Treaty.” J. Ashley Roach, *International Law and the Arctic: A Guide to Understanding the Issues*, 15 SW. J. INT’L L. 301, 319-20 (2009).

The United States has many reasons to make a commitment such as the one in Tromsø. First, the United States is an Arctic coastal nation with sovereign interests in the marine environment abutting its exclusive economic zone (“EEZ”) and territorial sea as well as within its continental shelf.²⁴ Second, strategic and national security interests proliferate as melting continues, with desire to ensure freedom of navigation within the Northern Sea Route and the Northwest Passage, prevention of a new avenue of ingress for terrorism, preservation of the marine environment, “project[ion] [of] a sovereign United States maritime presence in the Arctic . . . [and] [e]ncourag[ement] [of] the peaceful resolution of disputes in the Arctic region.”²⁵ Third, in addition to having Arctic circle inhabitants, the United States has undertaken actions in the Arctic through its various agencies for some time now. These include marine research, military activities, and regulation of U.S. shipping and marine resources.²⁶ In this vein, the federal agency employees who plan potential projects, seek necessary permits, and prepare for consultations under U.S. laws will need to take this strategy into account.

Without a treaty and implementing U.S. laws or guidance from the White House Council on Environmental Quality (“CEQ”) or another federal agency with expertise to provide to these federal planners, uncertainty exists as to how to proceed when an activity is planned in the “Arctic.”²⁷ Uncertainty arises when the planner attempts to determine which U.S. domestic environmental law to apply in the ocean waters of the Arctic. For instance, undertaking to evaluate the impacts of a U.S. Coast Guard search-and-rescue training exercise or a U.S. Navy submarine’s ice research in support of the National Science Foundation requires months of evaluation prior to the decision to engage in the specific activity in a specific location of water space in the Arctic. That evaluation

²⁴ See Directive on Arctic Region Policy, *supra* note 4.

²⁵ *Id.*

²⁶ See generally materials from various agencies, *for example*, U.S. Arctic Research Commission, <http://www.arctic.gov/about.html> (last visited Nov. 1, 2009); National Science Foundation, Office of Polar Programs, <http://www.nsf.gov/dir/index.jsp?org=OPP> (last visited Nov. 1, 2009); National Oceanic and Atmospheric Administration, <http://www.arctic.noaa.gov/> (last visited Nov. 1, 2009); David Kerley, Under the Ice in the Arctic: An Exclusive Look Inside the U.S. Navy’s Polar Environment Submariner Training, (Oct. 14, 2009), <http://abcnews.go.com/Politics/journey-arctic-exclusive-us-navys-polar-submariner-training/story?id=8168432>; U.S. Department of State, <http://www.state.gov/g/oes/ocns/opa/index.htm> (last visited Nov. 1, 2009); National Oceanic and Atmospheric Administration Fisheries, <http://www.alaskafisheries.noaa.gov/sustainablefisheries/arctic/> (last visited Nov. 1, 2009); U.S. Department of Transportation, Maritime Administration, http://www.marad.dot.gov/environment_safety_landing_page/arctic_transportation/Arctic_Transportation.htm (last visited Nov. 1, 2009).

²⁷ “Arctic” is used in the most general and broad sense here to connote the different jurisdictional boundaries of the activity. Further discussion follows below.

typically requires analysis under NEPA (or Executive Order 12114, which pertains to environmental effects abroad), under the MMPA, and under the ESA, at minimum. But while the mandates of those statutes may be clear, understanding where to apply them, from the territorial seas to the high seas or even a foreign nation's EEZ, is much less clear. Each statute has specific language denoting some limit to its application in United States territory out to territorial seas, waters of the United States, or even high seas. But no uniformity exists and courts faced with attempting to review agency actions for failure of some alleged violation of the NEPA, MMPA, or ESA have not established a clear stance on how far out these laws should intrude into the sovereign areas of other nations. Can the United States provide an MMPA permit for an activity in what is or may be settled upon as Russia's EEZ? And perhaps more importantly, should it? Does applying NEPA-like analysis to an activity on the high seas portion of the Arctic Ocean equate in analysis to applying NEPA for any major federal agency action in other territories, lands and waters of the United States? Will imposing terms and conditions within an incidental take statement of a biological opinion that necessitates ships or aircraft intruding into a still-under-dispute area of the Beaufort Sea between United States and Canada create international tension? And if the United States extends its laws extraterritorially then what is to stop other countries from attempting to do the same and require U.S. activities to also abide by required laws and terms, conditions, mitigation, or other parameters that country so chooses? These are some of the questions that an agency's environmental planner or lawyer must consider when preparing for a federal major action in the Arctic Ocean.

Extending any one or all of these domestic laws, as some advocates recommend, to the shores of another nation intrudes into the sovereignty of that nation over conservation of the marine environment and natural resources.²⁸ The Arctic's over-arching international cooperative efforts and entrenched sovereignty viewpoints create a backdrop where United States domestic law

²⁸ See generally Randall S. Abate, *Dawn of a New Era in the Extraterritorial Application of U.S. Environmental Statutes: A Proposal for an Integrated Judicial Standard Based on a Continuum of Context*, 31 COLUM. J. ENVTL. L. 87, 99 (2006); Paul Boudreaux, *Biodiversity and a New 'Best Case' for Applying the Environmental Statutes Extraterritorially*, 37 ENVTL. L. 1107 (2007); but see Keith S. Gibel, *Defined by the Law of the Sea: 'High Seas' in the Marine Mammal Protection Act and the Endangered Species Act*, 54 NAVAL L. REV. 1 (2007) (arguing that the MMPA and ESA do not apply in foreign exclusive economic zones because Congress' use of "high seas" in each act meant areas not subject to exercise of a foreign sovereign's rights as understood under international law and because authority for both laws stems from control over natural resources.); Dierdre Goldfarb, Comment, *NEPA: Application in the Territorial Seas, the Exclusive Economic Zone, the Global Commons, and Beyond*, 32 SW. U. L. REV. 735 (2003); Karen Klick, Note, *The Extraterritorial Reach of NEPA's EIS Requirement After Environmental Defense Fund v. Massey*, 44 AM. U. L. REV. 291, 319-321 (1994).

may have to acquiesce or flex to regional initiatives or agreements to preserve sovereignty agreed to under the UNCLOS.²⁹ The mandate of NEPA may require more heightened scrutiny of environmental impacts due to the unique Arctic conditions based on guidance that the Arctic Council has produced.³⁰ But there should not be a push to apply NEPA as opposed to the Executive Order 12114 analysis in foreign waters. Executive Order 12114 mandates “NEPA-like” analysis in these UNCLOS defined areas already in a manner that preserves and considers the sovereignty of other nations as well. Executive Order 12114 reflects the Executive Branch’s position that NEPA does not apply extraterritorially.³¹ It is an opinion that has not been rescinded or altered like other policy that suggested NEPA apply extraterritorially.³² The Executive Order “represents the United States government’s exclusive and complete determination of the procedural and other actions to be taken by Federal agencies to further the purpose of [NEPA], with respect to the environment outside the United States, its territories and possessions.”³³ It directs agencies to consider the effects of their actions “on the environment outside the geographic borders of the United States.”³⁴ The Executive Order balances the requirement to consider environmental effects with certain acts relating to national security, intelligence activities, nuclear activities, and arms transfers and allows for exemption of these acts from the requirements.³⁵ Additionally, agencies may modify the content, timing, and availability of the reports they are required to prepare when necessary to “avoid adverse impacts on foreign relations,” or because of “national security considerations.”³⁶ Ultimately, the balance incorporated into Executive Order 12114 reflects the constitutional commitment of foreign affairs and national defense to the President.

U.S. regulatory agencies overseeing implementation of the MMPA and ESA demonstrate willingness to stretch application of these statutes extraterritorially beyond their legislative intent in coverage limits.³⁷ Further, MMPA permits or ESA incidental take statements issued for activities in areas

²⁹ “The domestic legal responses of the Arctic states therefore have a major role to play in the Arctic Legal Regime. Nonetheless, this prevalence of Arctic domestic law has not prevented the development of an identifiable international law regime in the region.” DONALD R. ROTHWELL, *THE POLAR REGIONS AND THE DEVELOPMENT OF INTERNATIONAL LAW* 155 (1996).

³⁰ Arctic Environmental Protection Strategy, Guidelines For Environmental Impact Assessment (EIA) in the Arctic, <http://arcticcentre.ulapland.fi/aria/index.asp> (last visited Oct. 9, 2009).

³¹ See President Jimmy Carter, *Environmental Effects Abroad of Major Federal Actions*, E.O. 12114, 44 Fed. Reg. 1957 (Jan. 4, 1979).

³² See *infra* notes 125 -137 and accompanying text.

³³ *Id.* at § 1-1.

³⁴ *Id.* at §§ 2-1, 2-3.

³⁵ *Id.* at §§ 2-5(iii)-(v)

³⁶ *Id.* at § 2-5(b).

³⁷ See *infra* notes 200 - 204 & 211 - 218 and accompanying text.

under the sovereign control of other nations have potential to disrupt international goodwill in the Arctic where regional cooperation may be the best mechanism for handling marine environmental problems and ecosystem management and planning.³⁸

Therefore, this article's objective is to explain the current state of the demarcation of continental shelf claims and jurisdictional maritime boundaries related to the United States within the Arctic Ocean area and the application of certain U.S. environmental laws to activities within this still-shifting Arctic environment. This article is limited in scope to discussing domestic environmental law in relation to activities likely to be planned within the ocean expanse rather than land-based development or other terrestrial projects. Part II will set a backdrop of what kinds of federal agency actions take place in Arctic Ocean areas and why such activities take place. Part III will explain where boundary disputes currently lie in relation to United States interests. Part IV will then discuss where U.S. domestic laws,³⁹ particularly the NEPA, MMPA, and ESA, currently apply to federal "at-sea" activities in the Arctic. In Part V, the article will explore whether the reach of these domestic laws already is being extended and whether the presumption against extraterritoriality should control. Looking at the plain language and legislative history of the statutes, and applying the presumption against extraterritoriality, the article concludes that these federal laws should not be extended, given the Arctic's backdrop of varying jurisdictional boundaries and overlapping international cooperative scheme.

II. AGENCY ACTIONS IN THE ARCTIC SEAS

The relevance of this article rests first with having an understanding of which United States agencies are engaged in activities within the waters of the Arctic region and why there is likely to be more of a federal presence in the future. Looking at a few agency actions will help in this understanding.

The United States Coast Guard ("Coast Guard") has over 142 years of Arctic service, which includes mission responsibilities of maritime security and stability, homeland security, marine environmental response, ice operations (national security and scientific), maintaining aids of navigation (buoys and

³⁸ See generally Arctic Council, Tromso Declaration (Apr. 29, 2009), available at <http://arctic-council.org/filearchive/Tromsoe%20Declaration-1.pdf> (indicating desire for "growing cooperation among the Arctic States").

³⁹ Federal agencies have other federal regulations, laws and executive orders they must comply with when planning a proposed activity, but this paper is limited in scope to the three main environmental statutes and related regulations.

Loran stations), maritime law enforcement (monitoring the U.S.-Russian boundary line), and probably its most well-known mission of search and rescue operations.⁴⁰ With the changing ice and environmental conditions in the Arctic Ocean, including the 2008 summer sea ice minimum⁴¹ which opened both the Northern Sea Route (connecting the Pacific to the Atlantic Ocean via polar waters along the coast of Russia) and the Northwest Passage (extending from the Atlantic through Baffin Bay and the Canadian northern islands and into the Pacific ocean via the Bering Strait), the Coast Guard recognizes that its traditional missions will be pushing further north in Alaska and surrounding Arctic ocean space and that it will need icebreakers and other logistical support and forward operating bases.⁴² Expanding Coast Guard operations will likely require balance of development, environmental, and national security interests, as well as the concerns and interests of Arctic communities.

The U.S. Navy's presence in the Arctic began with the USS Nautilus's (SSN 571) submerged transpolar crossing in 1958.⁴³ Since then, U.S. Navy forces have utilized Arctic Ocean waters for transits, training, and operations in the region. Such training includes activities such as practice of maritime interdiction, search and rescue, and tactical interoperability with other countries,

⁴⁰ For information on Coast Guard operations in the Arctic, see U.S. Coast Guard Seventeenth District, "Arctic Overview," <http://www.uscg.mil/D17/ArcticOverview.pdf> (last visited Mar. 7, 2010).

⁴¹ The primary parameter for measuring the state of the Arctic sea ice cover through sea ice extent with the annual cycle being defined by March, when the ice is at the end of winter and its maximum extent and September when it reaches its annual minimum. See D. Perovich *et. Al.*, "Sea Ice Cover," (Oct. 19, 2009) available at <http://www.arctic.noaa.gov/reportcard/seai.html>. This minimum is commonly referred to as the summer sea ice minimum. See *id.*

⁴² See U.S. Coast Guard, *supra* note 40; David Gove, *Changes in the Arctic Environment—No Matter the Cause—Are a Great National Security Concern*, PROC. Feb. 2009. The Coast Guard currently has three icebreakers, although two (USCGC Polar Star (WAGB-10) and USCGC Polar Sea (WAGB-11)) "are the only two built to handle heavy ice" and are "near the end of their service life." *Id.*; see also Matthew R. Wald and Andrew C. Revkin, *New Coast Guard Task in Arctic's Warming Seas*, N.Y. TIMES, Oct. 19, 2007, available at <http://www.nytimes.com/2007/10/19/us/19arctic.html> (indicating that Arctic warming could create new search-and-rescue and environmental protection responsibilities for the Coast Guard). "The resulting increase in Arctic activity will mean a greater need for search and rescue capabilities and for environmental protection, Coast Guard officials say. In fact, Admiral [Thad] Allen says ship traffic could turn the Bering Strait into a choke point like the Strait of Gibraltar." Rebekah Gordon, *Allen: Six Polar Icebreakers Ideal for Maximum Arctic Presence*, INSIDE THE NAVY, July 20, 2009 (discussing the Commandant of the U.S. Coast Guard's remarks to Senate committee that six icebreakers would provide the optimal number for appropriate presence in Arctic region). Coast Guard District Seventeen envisions forward operating bases being established possibly on the Northern Slope and Western Alaska. See U.S. Coast Guard, *supra* note 40.

⁴³ For an account of the historical voyage, see History of USS NAUTILUS, <http://www.usnautilus.org/nautilus/index.shtml> (last visited Feb. 28, 2010).

such as Russia and Norway.⁴⁴ “U.S. force presence in other parts of the Arctic supports U.S. Combatant commanders and [supports] strategic deterrence. The U.S. submarine force, in particular, is prepared to operate in and project maritime power from the Arctic.”⁴⁵ The U.S. Navy also utilizes the Arctic for evaluating tactics, platforms, weapons systems, and other equipment. Under the governance of the U.S. Navy’s Arctic Submarine Laboratory,⁴⁶ which plans and coordinates the U.S. Navy’s submarine Arctic program, submarines have worked with scientists since the 1970s to “collect Arctic data in support of the scientific community [on a] . . . not to interfere basis with military missions and requirements.”⁴⁷ Commonly referred to as “ICEX,” this recurring training and research exercise generally consists of at-sea research performed by the submarine as well as temporary establishment of an ice station (including runway) on the surface of the sea ice. The goal is “to give[] the Navy’s submarine force the opportunity to develop and hone their Arctic operational and warfighting skills in order to meet the challenges of the Arctic’s unique operational environment.”⁴⁸ The Navy also oversees the National Ice Center, “a cooperative, interagency organization responsible for providing Arctic, Antarctic, and Great Lakes ice information to U.S. and allied armed forces, U.S. government agencies, and various segments of private industry.”⁴⁹ The National Ice Center generates “[r]eal-time global, regional, and tactical scale ice guidance products” to support navigation, climate research and military mission planning.⁵⁰ Further, the Arctic Ocean is viable for

submerged transits throughout the Northwest Passage and the Arctic region. The Arctic is a particularly advantageous pathway for shifting submarines between the Atlantic and Pacific fleets. Such transits are quicker, more cove[r]t, more

⁴⁴ In July 2008, the U.S. Navy took part in Northern Eagle, a 12-day trilateral exercise including the U.S., Russia and Norway. The exercise, held in the Norwegian and Barents Seas, focused on maritime interdiction operations to practice skills against piracy, search and rescue and tactical interoperability to improve maritime safety and security in Northern Europe. *See* Christopher Henry, Fleet Public Affairs Center Detachment Europe, USS Elrod Practices Boarding Procedures with Russian Federation Navy During Exercise Northern Eagle, July 24, 2008, <http://www.eucom.mil/English/FullStory.asp?art=%7B4FA9B498-0061-4F8A-8CC5-B3E01B0E2D89%7D>.

⁴⁵ Roach, *supra* note 23, at 312.

⁴⁶ The Navy’s Arctic Submarine Laboratory homepage can be found at <http://www.csp.navy.mil/asl/index.htm>.

⁴⁷ Roach, *supra* note 23, at 313.

⁴⁸ Rebekah Blowers, CNO Attends ICEX 2009 (Mar. 24, 2009), *available at* http://www.navy.mil/search/display.asp?story_id=43706.

⁴⁹ Interagency Arctic Research Committee, Arctic Research of the United States 97 (2006), *available at* <http://www.nsf.gov/pubs/2007/nsf07137/nsf07137.pdf>.

⁵⁰ *Id.*

fuel efficient, more cost effective and provide greater force protection in comparison to alternative transits through the Panama Canal.⁵¹

If climate change opens further parts of the Arctic Ocean to transit, the U.S. Navy will likely face “[n]ational and homeland security interests . . . in the region [that] would include early warning/missile defense, maritime presence and security, and freedom of navigation and over-flight.”⁵² Operating in the unique environment of the Arctic more frequently will require more ice-hardened ships and may with warming conditions create a more conventional Navy operating environment.⁵³

In addition to the Navy’s assistance in the research of the Arctic, the National Science Foundation (“NSF”)⁵⁴ implements the mandate of the Arctic Research and Policy Act of 1984 (“ARPA”),⁵⁵ which provides for a comprehensive national policy dealing with national research needs and objectives in the Arctic. The ARPA establishes an Arctic Research Commission (“ARC”) and an Interagency Arctic Research Policy Committee (“IARPC”) to help implement the Act. The National Science Foundation is the chair of the IARPC. The Foundation is one of twelve Federal agencies that sponsor or conduct arctic science, engineering, and related research and monitoring activities. The NSF’s primary focus is on research to benefit national defense, resources, health, and science. The NSF has had a particular scientific research focus on the Polar Regions due to its lead role as coordinator for U.S. research projects conducted as part of the International Polar Year (March 2007 to March 2009), which was designated by the International Council for Science and the World Meteorological Organization. The event included over 200 science projects undertaken by scientists from more than 60 nations “focusing on research disciplines, from geophysics and ecology to social science and

⁵¹ Roach, *supra* note 23, at 312.

⁵² David Gove, *Arctic Melt: Reopening a Naval Frontier?*, PROC. Feb. 2009.

⁵³ The U.S. Navy currently has no ice-hardened surface ships (destroyers or cruisers), nor icebreakers. “[A]ll of its icebreakers were transferred to the Coast Guard in 1966 In addition to thinking through how we adjust our shipbuilding emphasis to support such operations, the Navy should also be thinking strategically about building the necessary infrastructure to provide logistic support for the Arctic patrols, search and rescue capabilities, and shore based support activities.” *Id.*

⁵⁴ The National Science Foundation (“NSF”) is an independent federal agency created by Congress in 1950 “to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense” See National Science Foundation, <http://www.nsf.gov/about/> (last visited Sept. 25, 2009).

⁵⁵ Public Law 98-373, July 31, 1984, *amended by* Public Law 101-609, Nov. 16, 1990 (codified as amended at 15 U.S.C. §§ 4101-4111).

economics.”⁵⁶

Under the Department of Transportation is the U.S. Maritime Administration (“MARAD”), which oversees regulation of shipping and all waterborne transportation requirements in the United States.⁵⁷ With the possibility of opening the navigation routes of the Northwest Passage and the Northern Sea Route due to reduction in sea ice, shipping traffic in the Arctic could dramatically increase. This would require heightened assurance of the ability of ships to traverse through these difficult maritime waters. Between 1979 and 1986, after the prospect of offshore oil and gas leases being marketed, the MARAD embarked on research voyages to not only demonstrate the feasibility of icebreaking ships journeying along future Arctic routes, but also to “[d]efine environmental conditions along routes in the Bering, Chukchi and Beaufort seas; and, [o]btain data to improve design criteria for ice-capable ships and offshore structures.”⁵⁸ Today, MARAD is a member of a federal interagency team representing U.S. interests at the International Maritime Organization (“IMO”).⁵⁹ In a recently released report by the Arctic Council⁶⁰ assessing shipping capabilities and requirements in the Arctic, a finding about regulation of Arctic shipping concluded there are “no uniform, international standards for

⁵⁶ WMO & ICSU, THE SCOPE OF SCIENCE FOR INTERNATIONAL POLAR YEAR 2007-2009, at 5 (2007), available at http://ipy.arcticportal.org/images/uploads/LR*PolarBrochureScientific_IN.pdf. There are six themes to the research that include: status, change, global linkages, new frontiers, vantage point and the human dimension. See *id.* NSF notes “[p]rojects, which are expected to be interdisciplinary, will involve a pulse of activity during the IPY period; leave a legacy of infrastructure and data; expand international cooperation; engage the public in polar discovery; and help attract the next generation of scientists and engineers to polar research.” See National Science Foundation, International Polar Year Awards, http://www.nsf.gov/od/opp/ipy/ipy_awards_list.jsp (last visited Oct. 15, 2009). The time period of the International Polar year from March 2007 to March 2009 covers two annual biological cycles to allow for full and equal coverage of the Arctic and Antarctica. See About International Polar Year, <http://www.ipy.org/about-ipy> (last visited Mar. 7, 2010).

⁵⁷ As noted on its website,

[p]rograms of the Maritime Administration promote the development and maintenance of an adequate, well-balanced United States merchant marine, sufficient to carry the Nation's domestic waterborne commerce and a substantial portion of its waterborne foreign commerce, and capable of service as a naval and military auxiliary in time of war or national emergency. The [U.S.] Maritime Administration also seeks to ensure that the United States maintains adequate shipbuilding and repair services, efficient ports, effective intermodal water and land transportation systems, and reserve shipping capacity for use in time of national emergency.

U.S. Maritime Administration, http://www.marad.dot.gov/about_us_landing_page/marad_faq/FAQ.htm#q1 (last visited Aug. 5, 2009).

⁵⁸ ARCTIC COUNCIL, ARCTIC MARINE SHIPPING ASSESSMENT REPORT 47 (2009).

⁵⁹ See U.S. Maritime Administration, <http://www.marad.dot.gov>.

⁶⁰ See ARCTIC COUNCIL, *supra* note 58.

ice navigators and for Arctic safety and survival for seafarers in polar conditions. And, there are no specifically tailored, mandatory environmental standards developed by IMO for vessels operating in Arctic waters. Mandatory measures, drawn up in accordance with the provisions of customary international law as reflected in UNCLOS, would be an effective way to enhance marine safety and environmental protection in Arctic waters.”⁶¹

In addition to ensuring protection of marine species through permitting incidental takes of marine mammals and endangered and threatened marine species under the MMPA and ESA, the National Marine Fisheries Service (“NMFS”) and U.S. Fish and Wildlife Service (“FWS”) have an interest in protection of fisheries within the Arctic Ocean. In February 2009 the North Pacific Fishery Management Council recommended a fishery management plan for the Arctic, due to concerns about future opening of the ice-laden area within the U.S. EEZ to future commercial fishing.⁶² The plan covers the “Arctic Management Area,” which consists of currently closed U.S. EEZ areas of the Chukchi Sea and Beaufort Sea. Anticipating the need for management in the future, “[f]or Arctic fish resources, the policy is to prohibit all commercial harvests of fish until sufficient information is available to support the sustainable management of a commercial fishery.”⁶³ Sometimes NMFS and FWS, as resource managers within the Arctic waters, are the regulatory authorities for permitting other federal activities, and sometimes they are the action agencies when conducting their own activities, such as wildlife studies or setting fishing quotas.

These are just some of the federal agency activities that transpire in the Arctic Ocean. Oil and gas exploration and development on the Outer Continental Shelf through the programs supported by the Minerals Management Service are other significant activities being planned for in the Arctic. However, given the stationary nature and unique management system of the activity,⁶⁴ it is not further discussed in this paper. In sum, the Arctic is not a “no-man’s” land without activity. Human activity in the Arctic is anticipated on a greater scale in the future. Federal agencies will have continued interests in exploring, researching, training, traversing and protecting the Arctic Ocean. The challenge

⁶¹ *Id.* at 4.

⁶² The management plan is completed pursuant to the Magnuson-Stevens Fisheries Conservation and Management Act. With public comment having just closed, the management plan is currently still pending final approval of the Secretary of Commerce. *See* North Pacific Fishery Management Council, Fishery Management Plan for Fish Resources of the Arctic Management Area (Aug. 2009), <http://www.fakr.noaa.gov/npfmc/fmp/arctic/ArcticFMP.pdf>.

⁶³ *Id.* at ES-1.

⁶⁴ *See* Outer Continental Shelf Lands Act, 43 U.S.C.A. § 1301 *et seq.* (West 2009); *see also* Mineral Management Service, <http://www.mms.gov/alaska/lease/lease.htm>.

for the federal environmental planners will be how to ensure adherence to U.S. environmental laws and regulations when planning projects in the dynamic Arctic environment against a backdrop that favors international initiatives and collaboration in trying to maintain respect for the sovereignty of other nations.

III. ARCTIC BOUNDARY DISPUTES

Some disputes that the United States has in the Arctic Ocean with other nations over boundaries could create changes to where future federal activities occur. The United States recognizes that it is important to settle these boundary issues in order to promote its exercise of sovereign rights over natural resources and living marine species in certain areas and as “critical to [the] national interests in energy security, resource management, and environmental protection.”⁶⁵ One bilateral dispute is with Canada over where the boundary line of Canadian and United States waters exists within the Beaufort Sea.⁶⁶ The disputed area of overlap of the two nations’ claims is nearly 7,000 square nautical miles⁶⁷ off east Alaska, stretching northward to the Canadian Yukon. The UNCLOS allows each nation to determine the breadth of its territorial sea measured from a baseline (generally low water mark) out to 12 nautical miles. The Convention points out two potential methods for this determination, straight baselines or equidistance of points from baseline.⁶⁸ Straight baselines should be used for land that is deeply indented, has fringing islands or when the land along which the baseline lies is highly unstable.⁶⁹ Equidistance theory draws a median line by having every point equally distant from the nearest points on the baseline.⁷⁰ Article 15 of UNCLOS allows for the equidistance method in delimiting territorial sea between adjacent coasts.⁷¹ The United States’ position in the dispute with Canada rejects that the 1825 treaty between Great Britain and Russia meant to determine a maritime boundary in addition to the land boundary that ultimately determined the boundary between Alaska and the Yukon along the 141st meridian.⁷² Instead, the United States believes that the boundary

⁶⁵ See Directive on Arctic Region Policy, *supra* note 4.

⁶⁶ See Robert Dufresne, Law and Government Division, Parliamentary Information and Research Service, Controversial Canadian Claims over Arctic Waters and Maritime Zones (Jan. 10, 2008), available at <http://www2.parl.gc.ca/Content/LOP/ResearchPublications/prb0747-e.htm#endnote44>.

⁶⁷ See *id.*; see also International Boundary Research Unit, Durham University, Maritime Jurisdiction and Boundaries in the Arctic Region at n.6, <http://www.dur.ac.uk/ibru/resources/arctic/> (last visited Aug. 3, 2009). The disputed area is just slightly bigger than the State of New Jersey. See NATIONAL GEOGRAPHIC, ATLAS OF THE WORLD (8th ed. 2004), available at http://travel.nationalgeographic.com/places/states/state_newjersey.html (last visited Nov. 2, 2009).

⁶⁸ See UNCLOS, *supra* note 6, arts. 3-16.

⁶⁹ See UNCLOS, *supra* note 6, art. 7.

⁷⁰ See Dufresne, *supra* note 66.

⁷¹ See UNCLOS, *supra* note 6, art. 15.

⁷² See Dufresne, *supra* note 66.

should be demarcated based on equidistance principles rather than by straight line theory, so that the boundary line would be “considerably to the east of a line based on 141°W”⁷³ where there are known “oil, natural gas and other resources.”⁷⁴

Second, the United States has a maritime boundary dispute with Russia in the Bering and Chukchi Seas that also primarily deals with “the boundary created by the 1867 Convention ceding Alaska, and whether it had any bearing upon the Beaufort Sea maritime boundary.”⁷⁵ However, this dispute was somewhat settled by a 1990 agreement between the two countries where Russia agreed to the United States exercising EEZ jurisdiction within an “‘Eastern Special Area’ [that] lies more than 200 nm from the baseline of the [United States] but less than 200 nm from the baseline of Russia.”⁷⁶ While Russia’s parliament has not yet ratified the agreement, the countries have honored the agreement through diplomatic notes.⁷⁷

The recognition of the Northwest Passage either as an international strait as defined by Part III of UNCLOS or internal waters of Canada has also been contested between Canada and other countries, primarily the United States. In 1985, after a voyage of a United States Coast Guard icebreaker through the Northwest Passage without the consent of Canada, Canada announced that straight-line baselines, resulting in the linking of all the northernmost islands of the Canadian Arctic Archipelago, “would be proclaimed around the outer islands” of the archipelago thereby delimiting the archipelago and the Northwest

⁷³ ROTHWELL, *supra* note 29, at 176.

⁷⁴ Directive on Arctic Region Policy, *supra* note 4. Further,

Canada argues that the maritime boundary in the Beaufort Sea was delimited in the 1825 treaty between Great Britain and Russia defining the boundary between Alaska and the Yukon as following the 141°W meridian ‘as far as the frozen ocean.’ The United States argues that no maritime boundary has yet been defined and that the boundary should follow the median line between the two coastlines. The area of overlap between the two claims is more than 7,000 nm².

International Boundary Research Unit, *supra* note 67, at n.6. But the United States indicates on the official Department of State, Bureau of Oceans and International Environmental and Scientific Affairs website that the boundary dispute is not interfering with cooperative efforts between Canada and the United States “to collect data necessary to define the continental shelf.” Further, it is noted that “[w]hile the United States and Canada have yet to agree on a maritime boundary in the Beaufort Sea/Arctic Ocean, they will work out the maritime boundary on a bilateral basis at an appropriate time.” See U.S. State Department, Bureau of Oceans and International Environmental and Scientific Affairs, Fact Sheet: Extended Continental Shelf (Mar. 9, 2009), <http://www.state.gov/g/oes/rls/fs/2009/120185.htm> [hereinafter Fact Sheet].

⁷⁵ ROTHWELL, *supra* note 29, at 176.

⁷⁶ See International Boundary Research Unit, *supra* note 67, at n.7.

⁷⁷ See *id.*

Passage as internal waters.⁷⁸ But other countries see the Northwest Passage as an international strait in which foreign ships have a right of transit without need for notice, consent or approval.⁷⁹

Other maritime boundary issues that do not directly affect United States interests (for instance, overlapping Russian and Norway EEZ claims) as well as submissions to the Commission on the Limits of the Continental Shelf regarding the continental shelf beyond 200 nautical miles by various Arctic nations, will have an impact on applicable law and policy that federal agencies must follow when conducting activities within varying Arctic waters.⁸⁰

Together, these disputes require that agency planners take note of them where their activities are planned and at minimum coordinate with the Department of State's Office of Ocean and Polar Affairs to ensure planning takes into consideration the U.S. policy on the international level with the Arctic Council.⁸¹

IV. MARITIME ZONES UNDER INTERNATIONAL LAW

Even against a backdrop of international "soft" law such as the guidance of the Arctic Council and various bilateral and multi-lateral conventions and treaties, domestic law plays an integral part in maritime activities that occur in

⁷⁸ See Dufresne, *supra* note 66. Designating the waters as internal means that Canada can demand requests for permission to transit through the Northwest Passage. But arguments asserting that the Northwest Passage should be deemed an international strait claim that other states enjoy right of innocent passage or right of transit passage. See *id.* See also ROTHWELL, *supra* note 29, at 184-85; Suzanne LaLonde, "Arctic Waters: Cooperation or Competition," Remarks at Vanderbilt Journal of Transnational Law Symposium, "Mounting Tensions and Melting Ice: Exploring the Legal and Political Future of the Arctic" (Feb. 6, 2009) (video link at <http://law.vanderbilt.edu/vulsplayer.asp?vid=68>); see also generally ARCTIC COUNCIL, *supra* note 58, at 51.

⁷⁹ See International Boundary Research Unit, *supra* note 67, at n.10. "While the Northwest passage was under permanent ice cover, the debate was largely academic- but with the polar ice cap retreating and the Passage becoming increasingly navigable, the question of which legal regime applies has become increasingly pressing. Similar issues affect the straits of the 'Northeast Passage' around Russia's Arctic Coastline." *Id.*

⁸⁰ Detailed discussion of all the claims of other nations sought and agreed on is beyond the scope of this paper. But a brief graphic with text description is found at International Boundary Research Unit, *supra* note 67. For discussion of the boundary dispute in the Barents Sea between Russia and Norway, see ROBIN CHURCHILL & GEIR ULFSTEIN, MARINE MANAGEMENT IN DISPUTED AREAS: THE CASE OF THE BARENTS SEA (1992).

⁸¹ The Department of State's Office of Ocean and Polar Affairs is "responsible for formulating and implementing U.S. policy on international issues concerning the oceans, the Arctic, and Antarctica." See U.S. State Department, Office of Ocean and Polar Affairs, <http://www.state.gov/g/oes/ocns/opa/index.htm> (last visited Oct. 11, 2009).

the Arctic.⁸² Commonly, the regime in the Arctic is understood to be one where the

states possess different rights in regard to their areas of territorial sovereignty and jurisdictional competence. With respect to areas of territorial sovereignty, the states are in principle free to decide the content of all policies [that] affect the area. [When activities remain within this territorial area], this means that the content of all policies which cover these activities, for instance, defense policy, industrial policy, and environmental policy, are freely decided by the Arctic states . . . states are free to decide the level of requirements in the planning phase within the limits of international law.⁸³

However, in the maritime domain in the Arctic, the United States' "power of decision is limited to those areas of policy which are expressly permitted by the law of the sea for each different zone. [Then] [i]n these specific areas of policy, the Arctic states have rights similar to those they enjoy with respect to territorial sovereignty."⁸⁴ Given this mixture of application of international law and domestic law in the Arctic, domestic law does not often get highlighted in discussions about the Arctic and issues surrounding it. But, indeed, U.S. domestic law applies to some maritime activities by U.S. federal agencies. To articulate the scope of those domestic laws particular to maritime areas, a well-developed set of maritime zones has emerged out of UNCLOS.⁸⁵ These zones set parameters on a nation's ability to assert jurisdiction or sovereignty over activities within a particular parcel of any ocean. Therefore, a discussion of maritime zones is necessary to understand to what extent U.S. domestic law will apply and whether that application is appropriate.

⁸² "Domestic laws of the Arctic states provide the framework for environmental protection. Yet global treaties and norms increasingly influence the content of domestic laws, and so provide backdrop for domestic legal development." See NOWLAN, *supra* note 14, at 5; see also ROTHWELL, *supra* note 29, at 156; Alf Håkon Hoel, *Do We Need a New Legal Regime for the Arctic Ocean?*, 24 INT'L J. OF MARINE AND COASTAL LAW 443 (2009).

⁸³ TIMO KOIVUROVA, ENVIRONMENTAL IMPACT ASSESSMENT IN THE ARCTIC: A STUDY OF INTERNATIONAL LEGAL NORMS 139-40 (2002). Further, the United States' position noted by J. Ashley Roach, CAPT, JAGC, U.S. Navy (Ret.), Office of the Legal Adviser, U.S. Department of State, is that "there are many sources of international law that are applicable to the Arctic Ocean, and more importantly, available to enhance the security, environmental protection and safety of navigation of the Arctic Ocean. As a result [the United States does] not believe it is necessary to develop a new regime of laws for the Arctic, as some have suggested." Remarks of J. Ashley Roach, Office of the Legal Adviser, U.S. Department of State, *The Ice Is Melting: Climate Change in the Canadian North Contested Waters: Sovereignty, Security, Strategy* (Mar. 7, 2008).

⁸⁴ KOIVUROVA, *supra* note 83, at 139-40.

⁸⁵ See UNCLOS, *supra* note 6.

First, the territorial sea is the “narrow belt of ocean immediately seaward of the coast.” In Article 3 of UNCLOS, every state is entitled to establish this territorial sea up to 12 nautical miles from “baselines” established by the State.⁸⁶ In the territorial sea, a state may exercise all jurisdiction as it has in its internal waters, except that foreign vessels have a right of “innocent passage” and that no criminal jurisdiction can attach against that foreign vessel moving in innocent passage unless there is an effect on the coastal state.⁸⁷ Nevertheless, a coastal state can extend application of its domestic law within the territorial sea to both its citizens and foreigners.

The contiguous zone allows the coastal state to extend its exercise of control and jurisdiction out to 24 nautical miles for purposes of preventing violations of “customs, fiscal, immigration or sanitary laws and regulations within its territory or territorial sea.”⁸⁸ Foreign vessels enjoy freedom of navigation and are not required to meet an innocent passage test and aircraft do not have to seek permission for over-flight. This zone gives the United States certain rights, but “short of sovereignty.”⁸⁹

The third zone beyond the territorial sea but adjacent to it is the EEZ, a zone that is not to exceed 200 nautical miles from the coast.⁹⁰ In this zone, a coastal state has

sovereign rights for the purpose of exploring and exploiting, conserving and managing the natural resources, whether living or non-living, of the waters superjacent to the seabed and of the seabed and its subsoil, and with regard to other activities for the economic exploitation and exploration of the zone, such as the production of energy from the water, currents and winds.⁹¹

⁸⁶ D. BAUER ET AL., OCEAN AND COASTAL LAW AND POLICY 7 (2008); *see also* UNCLOS, *supra* note 6, art. 3. As technology has evolved, computers now prepare the outer limits of the territorial sea by constructing arcs from points on the baseline. “By definition there is only one possible outer limit of the territorial sea once its breadth is known and the baseline is established. Controversies over the seaward limits of the territorial sea, and most other offshore boundaries, are actually baseline controversies.” BAUER, *supra* note 86, at 7.

⁸⁷ *See* BAUER, *supra* note 86, at 7-8.

⁸⁸ UNCLOS, *supra* note 6, art. 33.

⁸⁹ Goldfarb, *supra* note 28, at 735, 748.

⁹⁰ UNCLOS, *supra* note 6, art. 55.

⁹¹ *Id.*, art. 56.

Additionally, the coastal state can build artificial installations or islands, perform marine research and take action to protect the marine environment within its EEZ.⁹² Interestingly, in the EEZ, “[c]oastal state control over natural resources is recognized, but navigation and over-flight not inconsistent with resource interest are not restricted.”⁹³ The United States does claim an EEZ extending 200 nautical miles.⁹⁴

The continental shelf is the “sea-bed and subsoil of the submarine areas that extend beyond [a coastal nation’s] territorial sea throughout the natural prolongation of its land territory [to the greater of] the outer edge of the continental margin or . . . 200 miles from . . . [its coast].”⁹⁵ The UNCLOS allows for coastal states to seek extension of their continental shelf rights up to a maximum of 350 nautical miles from its coast.⁹⁶ The coastal nation-state claiming the continental shelf has complete sovereignty over that area; in other words, it may explore and exploit the natural resources and may require other nations to obtain its permission to explore or exploit the resources on its continental shelf.⁹⁷ Despite a coastal state’s sovereign authority over natural resources on its continental shelf, UNCLOS does allow for the right to navigate the waters and airspace above the continental shelf free from being required to seek permission first.⁹⁸ Additionally, all states have the right to “lay submarine pipelines and cables on the continental shelf of another State.”⁹⁹ In 1945 the

⁹² *See id.*

⁹³ BAUER, *supra* note 86, at 9.

⁹⁴ Initially the United States created an exclusive fishery zone under the Magnuson Fishery Conservation and Management Act, but then later amended and ratified the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. §1801 *et seq.*, which became the United States’ implementing legislation for recognition of the EEZ. *See id.* Even prior to the Act’s amendment, President Reagan had proclaimed in 1983 the recognition of the United States EEZ. *See* Proclamation No. 5030, 48 Fed. Reg. 10,605 (1983).

⁹⁵ BAUER, *supra* note 86, at 9; UNCLOS, *supra* note 6, art. 76(1).

⁹⁶ *See* UNCLOS, *supra* note 6, art. 76(1). To date only Russia and Norway have submitted claims to extended continental shelf to the Commission on the Limits of Continental Shelf regarding the Arctic Ocean areas. *See* http://www.un.org/Depts/los/clcs_new/submissions_files/submission_nor.htm (last visited Aug. 10, 2009). The United States has yet to ratify the UN Convention on the Law of the Sea. When it does, it will then have ten years to submit its claim. But the United States is already conducting extensive research to prepare for its claim. *See* Fact Sheet, *supra* note 74.

⁹⁷ BAUER, *supra* note 86, at 10.

⁹⁸ UNCLOS, *supra* note 6, art. 78.

⁹⁹ *Id.* art. 79. The right to lay pipelines or submarine cables on another state’s continental shelf is only limited by “its right to take reasonable measures for the exploration of the continental shelf, the exploitation of its natural resources and the prevention, reduction and control of pollution from pipelines, the coastal

State may not impede the laying or maintenance of such cables or pipelines. The delineation of the course for the laying of such pipelines on the continental shelf is subject to the consent of the coastal State.” *Id.*

United States was the first nation to assert a claim over the resources on its continental shelf.¹⁰⁰ The international community later followed with recognition of such claims by signing the Convention on the Continental Shelf.¹⁰¹ Ultimately, the United States set up a “comprehensive scheme for the federal development of mineral resources seaward of the state grants to the edge of the continental shelf.”¹⁰²

The extended continental shelf is the portion of the continental shelf beyond the 200 nautical mile mark that may be established by adhering to certain criteria within UNCLOS. Article 76 limits any claim of extended continental shelf to 350 nautical miles from the baselines of the territorial sea.¹⁰³ The extended continental shelf is not “an extension of the EEZ, [although the continental shelf area lies coincident to the EEZ. Further,] [s]overeign rights that apply to the EEZ, especially the right to resources of the water column do not necessarily apply to the [extended continental shelf.]”¹⁰⁴ A coastal state has the ability to exercise the same sovereign rights over the extended continental shelf as it does over the already defined continental shelf.¹⁰⁵ Specifically, in the Arctic it is believed that five of the Arctic states, namely, Denmark, Norway, Russia, Canada and the United States have extended continental shelves within the Arctic Ocean.¹⁰⁶ As previously noted, some of these states have already submitted their claims.¹⁰⁷

Further away from land of any nation are the “high seas,” which are the waters seaward of all the previously discussed zones that “are open to the use of

¹⁰⁰ A presidential proclamation by President Harry Truman sealed the claim.

¹⁰¹ Convention on the Continental Shelf, Apr. 29, 1958, 15 U.S.T. 471, T.I.A.S. 5578, *available at* http://untreaty.un.org/ilc/texts/instruments/english/conventions/8_1_1958_continental_shelf.pdf.

¹⁰² BAUER, *supra* note 86, at 10; *see also* Outer Continental Shelf Lands Act, 43 U.S.C.A. §§ 1331 *et seq.* (West 2009).

¹⁰³ UNCLOS, *supra* note 6, art. 76.

¹⁰⁴ Fact Sheet, *supra* note 74. The United States has begun research to delineate the extended continental shelf and in July 2009 undertook a 42-day Arctic cruise in partnership with Canada to gather scientific data about the extended continental shelf and the Arctic seafloor. *See* U.S. Department of State, U.S. and Canada to Conduct 2nd Joint Survey of the Extended Continental Shelf in the Arctic (July 22, 2009), *available at* <http://www.state.gov/r/pa/prs/ps/2009/july/126336.htm>. Despite the United States’ non-ratification of UNCLOS presently, the United States’ research efforts are in preparation for when the United States does ratify the convention and is then able to submit its claims to extended continental shelf boundaries. Given efforts by countries that are already under deadlines for submissions, the United States is taking advantage of the opportunity to cooperate now to save time and money. *See* Fact Sheet, *supra* note 74. Per UNCLOS, the United States will have ten years from ratification to make a submission to the Commission. *See id.*

¹⁰⁵ *See supra* notes 95 - 102 and accompanying text.

¹⁰⁶ *See* Fact Sheet, *supra* note 74.

¹⁰⁷ *See supra* notes 7- 96 and accompanying text.

all nations.”¹⁰⁸ On the high seas, nations enjoy many freedoms including those of navigation, laying submarine cables, over-flight, constructing artificial islands and installations, fishing and scientific research.¹⁰⁹ The high seas are also reserved for “peaceful purposes.”¹¹⁰ Moreover, “[e]very state may control its own nationals, and flag vessels,” and Article 92 of the UNCLOS calls for every vessel to be subject to that flag state’s “exclusive jurisdiction on the high seas.”¹¹¹ But nation states also have a duty to cooperate with each other regarding conservation and management of living marine resources and marine mammals within the high seas.¹¹²

Finally, the seabed below the high seas is known under UNCLOS as the “Area.” The “Area” is beyond the limits of national jurisdiction, and its resources are “the common heritage of mankind,” that can only be developed under the supervision of the International Sea-bed Authority.¹¹³ This framework by UNCLOS provides a uniform definition of each area of the ocean space of the world and specifies the authority of nation states within the various areas of the oceans. Despite this understanding of terms on the international level, U.S. domestic laws have not always been enacted or applied with the same understanding.

V. CURRENT APPLICATION OF NEPA, ESA AND MMPA TO “AT-SEA” ACTIVITIES

With this general knowledge of the zones of maritime jurisdiction, U.S. domestic law must be assessed for applicability to activities within these zones. There is a legal understanding that “Congress has the authority to enforce its laws beyond the territorial boundaries of the United States.”¹¹⁴ However, the Supreme Court has noted that “[i]t is a longstanding principle of American law ‘that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.’”¹¹⁵ The Court’s test is to

see whether ‘language in the [relevant Act] gives any indication of congressional purpose to extend its coverage

¹⁰⁸ BAUER, *supra* note 86, at 10.

¹⁰⁹ *See id.*; *see also* UNCLOS, *supra* note 6, art. 87.

¹¹⁰ UNCLOS, *supra* note 6, art. 88.

¹¹¹ BAUER, *supra* note 86, at 10; UNCLOS, *supra* note 6, art. 92.

¹¹² *See* UNCLOS, *supra* note 6, arts. 65, 117-120.

¹¹³ BAUER, *supra* note 86, at 10-11. Further discussion of the “Area” is beyond the scope of this paper.

¹¹⁴ *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991).

¹¹⁵ *Id.* at 248 (quoting *Foley Bros. v. Filardo*, 336 U.S. 281, 284-285 (1949)).

beyond places over which the United States has sovereignty or has some measure of legislative control . . . [and] unless there is ‘the affirmative intention of the Congress clearly expressed,’ . . . [the Court] must presume it ‘is primarily concerned with domestic conditions.’¹¹⁶

The reluctance of the Court to apply U.S. law outside the territorial jurisdiction of the United States is meant to “protect against unintended clashes between [U.S.] laws and those of other nations which could result in international discord.”¹¹⁷ While this test seems straightforward, the Supreme Court has muddled the application of the presumption through subsequent case law. Particularly, it has shifted from requiring a “clear statement” or “a plain statement of extraterritorial statutory effect”¹¹⁸ within the statutory text to instead looking for “‘clear evidence’ of congressional intent,”¹¹⁹ which includes “all available evidence . . . including text, structure, and legislative history to find ‘the affirmative evidence of intended extraterritorial application’”¹²⁰ At least one circuit court has noted this change in analysis. In finding that the Comprehensive Environmental Response, Compensation, and Liability Act (“CERCLA”) does not apply extraterritorially, so that environmental groups could petition to have the United States conduct preliminary assessments at two former military bases outside of the territory of the United States, the Ninth Circuit in *Arc Ecology v. United States Air Force* indicated that the change from requiring a direct statement in the text of a statute to “clear evidence” gives greater leeway to lower courts “in determining whether Congress intended to override the presumption against extraterritoriality.”¹²¹ Therefore, lower courts’ findings have inconsistently applied the presumption against extraterritoriality and have created varying tests. For example, the “conduct test” favors not applying the presumption when a statute pertains to “conduct regulated by the government [that] occurs within the United States,” while the “effects test” overcomes the presumption against extraterritorial application if the

¹¹⁶ *Id.* (quoting *Foley Bros. v. Filardo*, 336 U.S. 281, 284-285 (1949) and *Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957)).

¹¹⁷ *Id.*; see also *McCulloch v. Sociedad Nacional de Marineros de Honduras*, 372 U.S. 10, 20-22 (1963).

¹¹⁸ *Astoria Fed. Savings & Loan Ass’n v. Solimino*, 501 U.S. 104, 109 (1991).

¹¹⁹ *Smith v. United States*, 507 U.S. 197 (1993).

¹²⁰ *Abate*, *supra* note 28, at 87, 99 (citing *Sale v. Haitian Centers Council, Inc.*, 509 U.S. 155 (1993)). In *Sale*, the Court noted that “the presumption has special force when we are constructing . . . statutory provisions that may involve foreign and military affairs for which the President has unique responsibility.” *Id.*

¹²¹ *Arc Ecology v. United States Air Force*, 411 F.3d 1092, 1098 fn.2 (9th Cir. 2005).

presumption would result in undesirable effects within the United States.¹²² Application of the presumption to the three main U.S. environmental statutes (NEPA, MMPA, and ESA) has led to varying determinations, as will be discussed below. Given the role of U.S. federal agencies in Arctic activities and the varying areas where those activities could be conducted, the presumption against extraterritoriality should be kept in mind when considering the extent of application of these statutes to Arctic maritime activities.

A. NEPA and Executive Order 12114 application

Whether it is Coast Guard search and rescue efforts, Navy submarine research assistance, or MARAD ships engaged in international trade, federal agencies are engaged in activities in the Arctic requiring assessment of whether NEPA or NEPA-like analysis applies and to what extent. NEPA requires that federal agencies consider the environmental effects of their actions before taking actions. Therefore, an environmental impact statement (“EIS”) must be prepared before “every . . . major Federal action[] significantly affecting the quality of the human environment.”¹²³ The purpose of the EIS is to be an “action-forcing” device in order to provide “full and fair discussion of significant environmental impacts and . . . [to] inform decision makers and the public of reasonable alternatives which would avoid or minimize adverse impacts or enhance the quality of the human environment.”¹²⁴ Determining where NEPA applies in the context of various maritime zones is not clarified by the text of the statute, through legislative history or even clearly through case law. The statute is silent as to the geographic extent of its application.¹²⁵ Council on Environmental Quality (“CEQ”) regulations post-enactment of NEPA are also silent on clarifying NEPA’s scope of applicability outside the territory of the United States.¹²⁶ CEQ has only made some less direct, formal statements. After issuing initial guidelines to federal agencies on how to implement NEPA in 1971, CEQ eventually promulgated formal guidelines.¹²⁷ They were codified in the Code of Federal Regulations and indicated that in taking into account the impacts on the environment of the proposed major federal action, an agency needed to take into account the “positive and negative effects of the proposed action as it affects

¹²² Abate, *supra* note 28, at 100 & n.72 (describing the varying circuit court “effects” tests and “conduct” test, primarily in relation to application of economic regulation); *see also* Klick, *supra* note 28; Boudreaux, *supra* note 28.

¹²³ 16 U.S.C.A. § 4332 (West 2009).

¹²⁴ 40 C.F.R. § 1502.1 (1992).

¹²⁵ *See* Goldfarb, *supra* note 28, at 738.

¹²⁶ *See* 40 C.F.R. Parts 1500-1508 (2008).

¹²⁷ *See* 40 C.F.R. § 1500.8(a)(3) (1973).

both the national and international environment.”¹²⁸ This at least suggested some extraterritorial effect. And in September 1976, CEQ Chairman Russell Peterson issued a memorandum outlining why CEQ believed that NEPA applied to all significant effects of proposed major federal actions in the United States and “in other countries and in areas outside the jurisdiction of any country.”¹²⁹ He explained that the “human environment” in NEPA should not be limited and that, in as much as the term is unlimited in the statute, to view it in a broad application would conform with the mandate in Section 102(2)(C) to all agencies to “recognize the worldwide and long range character of environmental problems.”¹³⁰ This opinion was followed by CEQ proposing draft regulations to apply NEPA to federal projects outside of the United States.¹³¹ These draft regulations required agencies to file a “Foreign Environmental Impact Statement” for major actions outside the United States that affected the environments of one or more foreign countries.¹³² Otherwise, the draft regulations required adherence to NEPA regulations for actions within the United States and trust territories, global commons, and Antarctica that had a significant effect on the environment.¹³³ “Global commons” in these draft regulations suggested coverage of activities within the world’s oceans by indicating the term referred to areas “outside the jurisdiction of any nations (e.g. the oceans).”¹³⁴

However, by May 1978, CEQ decided to alter guidance to agencies with more formal procedural regulations and withdrew these draft regulations requiring NEPA to be conducted outside the territory of the United States, and the concept of a foreign environmental impact statement. Through the new proposed regulations in 1978, CEQ identified internal conflict within the government over how far NEPA should extend and concluded that “[n]othing in these regulations should be construed as asserting that NEPA either does or does

¹²⁸ *Id.*; see also 38 Fed. Reg. 20550 (Aug. 1, 1973) (making these revised guidelines applicable to all EISs prepared after Jan. 23, 1973).

¹²⁹ Russell W. Peterson, CEQ Chairman, Memorandum on the Application of the EIS Requirement to Environmental Impacts Abroad of Major Federal Actions (September 24, 1976), *reprinted in* 42 Fed. Reg. 61068-61069 (Dec. 1, 1977).

¹³⁰ *Id.*; see also Klick, *supra* note 28, at 299-300.

¹³¹ See CEQ Memorandum to Agency Heads on Overseas Application of NEPA Regulations (Jan. 19, 1978), *reprinted in* 8 Env’t Rep. (BNA) 1493 (1978); see also CEQ Draft Regulations on Applying NEPA to Significant Foreign Environmental Effects (1978), *reprinted in* 8 Env’t Rep. (BNA) 1495 (1978).

¹³² See CEQ Draft Regulations on Applying NEPA to Significant Foreign Environmental Effects (1978), *reprinted in* 8 Env’t Rep. (BNA) 1495 (1978).

¹³³ See CEQ Draft Regulations on Applying NEPA to Significant Foreign Environmental Effects (1978), *reprinted in* 8 Env’t Rep. (BNA) 1495 (1978).

¹³⁴ *Id.*

not apply [to effects occurring outside of the United States].”¹³⁵ To the present day, CEQ’s NEPA regulations are silent on whether to apply NEPA beyond U.S. territory.¹³⁶ Seemingly, the withdrawal of these draft regulations suggesting NEPA applied outside the territory of the United States is an indication that the agency charged with applying NEPA (CEQ) chose not to extend the law extraterritorially. CEQ’s only comment since 1978 about the scope of applicability of the law outside the territory of the United States is discussion of transboundary effects of activities within the United States, its territories, or its possessions. It noted that its guidance was not intending to “apply NEPA to so-called ‘extraterritorial actions’; that is, U.S. actions that take place in another country or otherwise outside the jurisdiction of the United States.”¹³⁷ Executive Order 12114 is still the applicable guidance absent NEPA application for agencies on assessing environmental impacts of federal actions outside of the territory of the United States.¹³⁸ Given NEPA’s silence on extraterritoriality and CEQ’s reversal in promulgating regulations interpreting NEPA extraterritorially, courts have tackled the issue even despite the Executive Order policy.

The Court of Appeals for the District of Columbia is the only circuit court that has addressed NEPA’s extraterritoriality.¹³⁹ The D.C. Circuit first addressed NEPA’s application outside the United States in *Natural Resource Defense Council v. Nuclear Regulatory Commission* in 1981.¹⁴⁰ In this decision, the D.C. Circuit ruled that NEPA does not apply to nuclear export licensing decisions by the Nuclear Regulatory Commission in face of environmental concerns of the shipment of a nuclear reactor to the Philippines that had significant impacts on that country but no impact within the United States.¹⁴¹ The court limited its ruling to the factual scenario before it (nuclear exports), and determined that in light of foreign policy and nonproliferation objectives of the United States, NEPA’s language noting that agencies should recognize the worldwide character of environmental problems consistent with foreign policy meant to promote consistent cooperative action rather than unilateral EIS judicial review.¹⁴² Therefore, the Court found that “NEPA’s putative extra-territorial reach [should] be curbed in the case of nuclear exports.”¹⁴³ Over ten years later

¹³⁵ 43 Fed. Reg. 25,230, 25,232 (June 8, 1978).

¹³⁶ See Council on Environmental Quality, 40 C.F.R. §1500.1-1500.18 (2009).

¹³⁷ Kathleen A. McGinty, CEQ Chairman, Memorandum to Heads of Agencies on the Application of the National Environmental Policy Act to the Proposed Federal Actions in the United States with Transboundary Effects (July 1, 1997), available at <http://ceq.hss.doe.gov/nepa/regs/transguide.html>.

¹³⁸ See *supra* notes 31-36 and accompanying text.

¹³⁹ See *Env’tl. Def. Fund, Inc. v. Massey*, 986 F.2d 528 (D.C. Cir. 1993).

¹⁴⁰ 647 F.2d 1345 (D.C. Cir. 1981).

¹⁴¹ See *id.* at 1366.

¹⁴² See *id.*

¹⁴³ *Id.* at 1348 (referring to NEPA § 102(2)(f)).

in 1993, the D.C. Circuit addressed NEPA and the presumption against extraterritoriality again in *Environmental Defense Fund, Inc. v. Massey* when it found that NEPA applied to the incineration of food waste in Antarctica.¹⁴⁴ In reaching the conclusion, the D.C. Circuit found that the presumption against extraterritoriality did not apply because the regulated conduct (application of NEPA) was the agency's decision-making process which occurs completely within the United States, the effect of that conduct is felt on Antarctica, a continent without a sovereign but one over which the United States "has a great measure of legislative control," and there is no apparent conflict with laws of other countries.¹⁴⁵ The *Massey* court indicated that "since NEPA is designed to regulate conduct occurring within the territory of the United States, and imposes no substantive requirements which could be interpreted to govern conduct abroad, the presumption . . . does not apply."¹⁴⁶ The *Massey* court relied on previous Supreme Court application of the presumption to explain that where the United States has "some measure of legislative control" the presumption against extraterritoriality is weaker.¹⁴⁷ Then the court noted that if there is no "potential for conflict between [United States] laws and those of other nations" then the purpose of the presumption disappears and it applies, if at all, with "significantly less force."¹⁴⁸ However, shortly after this case was decided, the Supreme Court decided another case in March 1993 pertaining to application of U.S. law within Antarctica in *Smith v. United States*.¹⁴⁹ In that case, the Court determined that the Federal Tort Claims Act's foreign country exception applied even to Antarctica, a sovereign-less region, to bar the wrongful death claim of a widower of a contractor for the federal government working in Antarctica.¹⁵⁰ The Court's decision was rooted not only in the plain language of the statute, but also the presumption against extraterritoriality.¹⁵¹ In the decision, the Court rejected the argument that the presumption should not apply to a sovereign-less place such as Antarctica since unintended clashes between the laws of the United States and those of other nations are not likely to occur and create international discord.¹⁵² Rather, the Court noted, "the presumption is rooted in a number of considerations, not the least of which is the commonsense notion that Congress generally legislates with domestic concerns in mind."¹⁵³ Therefore,

¹⁴⁴ *See id.*

¹⁴⁵ *Massey*, 647 F.2d at 533-34 (citing EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991)).

¹⁴⁶ *Id.* at 533.

¹⁴⁷ *Id.* at 533-34 (citing *Arabian American Oil Co.*, 499 U.S. at 248).

¹⁴⁸ *Id.* at 533.

¹⁴⁹ *See Smith v. United States*, 507 U.S. 197 (1993)). This decision did not mention the D.C. Circuit's opinion in *Massey*.

¹⁵⁰ *See id.* at 205.

¹⁵¹ *See id.* at 200-205.

¹⁵² *See id.* at 204 & n.5.

¹⁵³ *Id.* at 205.

while conflicts of law which create international discord are one reason to apply the presumption against extraterritoriality, the Supreme Court has held that the presumption has a broader foundation.¹⁵⁴

The D.C. District Court had an opportunity to deal with NEPA and the presumption against extraterritoriality later that same year, in November 1993, in *NEPA Coalition of Japan v. Aspin*.¹⁵⁵ Despite the D.C. Circuit's ruling in *Massey*, the District Court found the presumption against extraterritoriality applicable when it decided that activities at United States military bases in Japan were not subject to NEPA review because there was a substantial likelihood of an effect on treaty relations with Japan and because foreign policy interests outweighed the benefit of preparing an EIS.¹⁵⁶ The District Court recognized the Supreme Court precedents (*Sale v. Haitian Centers Council* and *Small v. United States*) had noted that the presumption has broader application than just to situations where laws of nations conflict, and also noted that the presumption can apply to procedural aspects of a statute even if no conflict of law exists.¹⁵⁷ Nevertheless, the District Court did find conflict could occur due to longstanding treaties between Japan and the United States.¹⁵⁸ The court explained that

[t]he preparation of an EIS would necessarily require DOD to collect environmental data from surrounding residential and industrial complexes, thereby intruding on Japanese sovereignty. In addition, the DOD would have to [assess] the impact of Japanese military activities at these bases. There is no evidence that Congress intended NEPA to encompass the activities of a foreign sovereign within its own territory.¹⁵⁹

Other lower courts have reached similar conclusions when actions are occurring within the territory of another country.¹⁶⁰

This case law demonstrates that the presumption against extraterritoriality is

¹⁵⁴ See *Sale v. Haitian Centers Council*, 509 U.S. 155, 174 (1993) (citing *Smith v. United States*, 507 U.S. 197 (1993)).

¹⁵⁵ See *NEPA Coal. of Japan v. Aspin*, 837 F. Supp. 466 (D.D.C. 1993).

¹⁵⁶ See *id.*

¹⁵⁷ See *id.* at 466 & n.3.

¹⁵⁸ See *id.* at 467.

¹⁵⁹ *Id.* at 467 & n.5

¹⁶⁰ See *Greenpeace USA v. Stone*, 748 F. Supp. 749 (D. Haw. 1990) (finding that NEPA didn't apply to removal of munitions from stockpile and transportation with Germany because of a cooperative agreement between Germany and the United States, and noting that NEPA application would result in lack of respect for German sovereignty over actions occurring in Germany).

applicable to a procedural statute such as NEPA when there is a foreign policy implication or conflict with the law of another nation. Given this precedent, if a federal agency plans to conduct an activity on, for instance, Wrangel Island, an island lying off Russia's Arctic coast, a NEPA analysis would require data collection and likely public participation in Russia that could intrude upon the sovereignty of Russia even if that NEPA decision-making was primarily made within the United States and would have little effect on United States territory. Further, Russia likely has an environmental law similar to NEPA. For the reasons noted by the various courts, the presumption against extraterritoriality should apply to limit NEPA in this hypothetical. But whether the presumption would apply to an activity within the *waters* surrounding Wrangel Island (within the Russian Exclusive Economic Zone) requires a look at whether U.S. courts have applied NEPA extraterritorially to maritime areas.

A few U.S. courts have addressed the scope of NEPA in offshore areas, and their conclusions differ. One case, *Basel Action Network and Sierra Club. v. Maritime Administration*, addressed the need for NEPA analysis in an action that included towing of de-commissioned naval ships across the high seas.¹⁶¹ In *Basel Action Network*, environmental groups sought to enjoin the towing of obsolete vessels from the James River Reserve Fleet in Virginia to the United Kingdom.¹⁶² The Maritime Administration had prepared an environmental assessment ("EA") and issued a finding of no significant impact ("FONSI") for the towing activities that encompassed the towing on the James River, Chesapeake Bay, and Atlantic coastline "to the seaward extent of U.S. Territorial Waters."¹⁶³ Sierra Club challenged the adequacy of the EA and argued that it failed to analyze the impacts of towing the ships across the high seas, among other claims.¹⁶⁴ Ultimately, in deciding that MARAD was not required to consider the effects of the towing across the high seas in this NEPA analysis, the court relied on the presumption against extraterritoriality.¹⁶⁵ It did so, fully acknowledging the decision of the *Massey* court and the D.C. Circuit Court's four reasons: In *Massey*, the decision-making was in the United States; the United States does not have legislative control over Antarctica; there was no potential for conflict with laws of other countries; and the presumption applies with less force in sovereign-less areas.¹⁶⁶ But the district court found *Massey* distinguishable primarily because the Supreme Court had ruled since *Massey*

¹⁶¹ 370 F. Supp. 2d 57 (D.D.C. 2005).

¹⁶² *See id.* at 62-63. Basel Action Network was ultimately found not to have standing to sue and therefore the case proceeded only with the claims of Sierra Club. *See id.* at 70.

¹⁶³ *Id.* at 71.

¹⁶⁴ *See id.* at 71.

¹⁶⁵ *See Basel Action Network*, 370 F.Supp. at 71-72.

¹⁶⁶ *See id.* at 71-72.

that the presumption against extraterritoriality still applies even when there is no clash of laws likely to occur.¹⁶⁷ Therefore, the district court found the decision-making to tow the vessels to the United Kingdom did occur by MARAD in the United States and applying NEPA on the high seas would probably not result in conflict with another nation's laws.¹⁶⁸ But the court acknowledged that the United States does not have legislative control over the high seas.¹⁶⁹ Since the Supreme Court instructed that the presumption against extraterritoriality should apply with equal vigor in areas with no sovereign, the District Court choose to still apply the presumption and found the EA's lack of analysis of impacts on the high seas was compliant with the law and dismissed the NEPA claim.¹⁷⁰

However, before *Basel Action Network*, the District Court of the Northern District of California issued a temporary restraining order for failing to comply with NEPA and MMPA prior to conducting acoustic research in the Gulf of California (within the Mexican EEZ), finding that "high seas" includes the EEZ.¹⁷¹ Despite "high seas" not being defined within either NEPA or MMPA, the district court in this case, *Center for Biological Diversity v. National Science Foundation*, drew on a couple of definitions of the "high seas" in federal law, regulations and the Geneva Convention on the High Seas.¹⁷² All of those definitions made no mention of the concept of EEZ.¹⁷³ And, interestingly, the court did not mention UNCLOS, which at the time of the ruling had been signed but not yet ratified by the United States and was in force among other nations.¹⁷⁴ Instead, the District Court determined that because the concept of "Exclusive Economic Zone" came into existence after the enactment of NEPA, the Gulf of California (an area within the Mexican EEZ) was not beyond the reach of NEPA application. Therefore, the District Court concluded that the area in question (the Gulf of California, part of the Mexican EEZ) was "territory which belongs to all nations but subject to the sovereignty of none . . . [the area was] explicitly found to be subject to . . . NEPA."¹⁷⁵ Interestingly, one of the laws the district court

¹⁶⁷ See *id.* at 72.

¹⁶⁸ See *id.*

¹⁶⁹ See *id.*

¹⁷⁰ See *Basel Action Network*, 370 F.Supp. at 72, 75; see also *supra* notes 149-154 and accompanying text.

¹⁷¹ 2002 U.S. Dist. LEXIS 22315 *1, *9-10 (N.D. Cal. 2002).

¹⁷² See *id.* at *9 & n.5.

¹⁷³ See *id.*

¹⁷⁴ See *id.*; see also generally Holmes, *supra* note 15, at 330-31 (noting that the United States signed the UNCLOS in 1994, the same year it entered into force, but the U.S. Senate has never ratified the convention).

¹⁷⁵ 2002 U.S. Dist. LEXIS 22315 at *9. This case is of limited import given the District Court's flawed analysis to derive that NEPA applies due to the EEZ equating to the high seas. But, it is included to be thorough in review of the applicable case law. For a detailed discussion of why the analysis is flawed, see Gibel, *supra* note 28, at 48-49.

looked to for the term “high seas,” the Magnuson-Stevens Fishery Conservation and Management Act, also contained a definition for “waters of a foreign nation” which defined the term as “any part of the territorial sea or exclusive economic zone (or the equivalent) of a foreign nation, to the extent such territorial sea or exclusive economic zone is recognized by the United States.”¹⁷⁶ It is not clear if the district court considered but discounted UNCLOS or this other definition against the high seas definitions it ultimately mentioned.

But just a month before the *CBD v. NSF* decision in the District Court of the Northern District of California, the District Court in the Central District of California ruled to apply NEPA within the United States’ EEZ in *NRDC v. Navy*.¹⁷⁷ In that case, the district court found that the United States’ substantial legislative control over the EEZ, to some extent “stemming from its ‘sovereign rights’ for the purpose of conserving and managing natural resources,” showed evidence that “NEPA applies to federal actions which may affect the environment in the EEZ.”¹⁷⁸ The district found that the EEZ is “not part of the territory of the United States, or under its exclusive legislative control”¹⁷⁹ but rather, based on the United States EEZ Proclamation, an area that is “beyond the territory and territorial sea of the United States in which all States enjoy the high seas freedom of navigation, overflight, the laying of submarine cables and pipelines, and other internationally lawful uses of the sea.”¹⁸⁰

Yet another court, the District Court of Hawaii, has also discussed the presumption against extraterritoriality and NEPA. In *Greenpeace U.S.A. v. Stone*, the court ruled that NEPA does not apply to the movement of munitions through and within West Germany and in transoceanic shipment to Johnston Atoll.¹⁸¹ With respect to the activities through and within Germany in support of transporting the munitions, the court found that NEPA application would not respect German sovereignty over actions occurring within that nation with which the United States had an existing cooperative agreement.¹⁸² For the transoceanic shipment, the Army had prepared a “Global Commons Environmental Assessment” per Executive Order 12114 while it prepared more than one EIS for other facets of the transport and ultimate destruction of the

¹⁷⁶ See 16 U.S.C.A. § 1802 (West 2009). The term “waters of a foreign nation” was added in 1990 so it was within the text of the version the district court would have reviewed. See Fishery Conservation Amendments of 1990, 101 Pub. L. 627, 104 Stat. 4436 (codified as amended at 16 U.S.C.A. § 1802 *et seq.* (West 2009)).

¹⁷⁷ See 2002 U.S. Dist. LEXIS 26360 *1, *41-42 (C.D. Cal. 2002).

¹⁷⁸ *Id.*

¹⁷⁹ *Id.* at *39.

¹⁸⁰ See *id.*; see also Proclamation No. 5030, 48 Fed. Reg. 10,605 (1983).

¹⁸¹ *Greenpeace U.S.A. v. Stone*, 748 F. Supp. 749 (D. Haw. 1990).

¹⁸² See *id.* at 32-33.

munitions.¹⁸³ Given the extent of that overseas EA, the District Court found that the specific facts of the case warranted finding that the Army had not violated NEPA by preparing the separate documents.¹⁸⁴ Therefore, at least in the Ninth Circuit, two district courts have decided to apply NEPA to major federal actions in both the U.S. EEZ and the Mexican EEZ, and one court has decided to allow only Executive Order 12114 analysis when the action takes place within various maritime zones.

Based on this case law, there is no definitive answer as to whether NEPA, as opposed to Executive Order 12114, must apply to federal activities in the contiguous zone, and in the U.S. EEZ beyond the 12 nautical mile territorial sea boundary, on the high seas, in a foreign EEZ, or in a foreign territorial sea. Legal scholarship and student articles on the subject have argued that NEPA should apply not only in the territorial seas but also in the EEZ, on the high seas and beyond.¹⁸⁵ These arguments for extending NEPA are made without regard to the fact that Executive Order 12114¹⁸⁶ exists to guide agencies. While Executive Order 12114 does not preempt application of NEPA to all federal agency actions taken outside the United States, compliance with the Order may be persuasive to a court in a particular circumstance to not extend NEPA extraterritorially.¹⁸⁷ Executive Order 12114, signed by President Carter in 1979, requires federal agencies to have procedures in place to “further the purpose of [NEPA], with respect to the environment outside the United States, its territories and possessions.”¹⁸⁸ The order calls for analysis of environmental impacts when major federal action has a significant effect on global commons outside the jurisdiction of any nation, on the environment of a foreign nation not participating with the United States in that action, on the environment of a

¹⁸³ See *id.* at 38-39.

¹⁸⁴ See *id.* at 40.

¹⁸⁵ See Abate, *supra* note 28 (proposing an integrated judicial standard based on the continuum of context in application of the presumption against extraterritoriality); Goldfarb, *supra* note 28, at 760-61 (proposing a broad uniform standard for NEPA application which includes extending NEPA through the global commons as well as within Foreign Exclusive Economic Zones and even foreign territories). “Any area where the United States exerts significant legislative control should be categorically within NEPA review, meaning the presumption against extraterritorial application should never apply and it should not be determined on a case-by-case basis.” *Id.* at 755; see also Klick, *supra* note 28, at 319-321 (recommending NEPA be amended to apply extraterritorially with one exemption for national security purposes only).

¹⁸⁶ Executive Order 12114, Environmental Effects Abroad of Major Federal Actions, 44 Fed. Reg. 1957 (Jan. 4, 1979).

¹⁸⁷ See *Greenpeace USA v. Stone*, 748 F. Supp. 749 (D. Haw. 1990) (citing *Indep. Meat Packers Ass’n v. Butz*, 526 F.2d. 228, 236 (8th Cir. 1975) (holding that Executive Order 12114, as a presidential order not issued pursuant to Congressional mandate, cannot preempt NEPA since it does not have the force and effect of law)). Further, Executive Order 12114 specifically notes that “nothing in this order shall be construed to create a cause of action.” 44 Fed. Reg. 1957.

¹⁸⁸ 44 Fed. Reg. 1957.

foreign nation when the United States is providing a product having a toxic effect that could create a serious public health risk or which is “strictly regulated by Federal law to protect the environment against radioactive substances,” or on “natural or ecological resources of global importance designated for protection under this subsection by the President or, in the case of such a resource protected by international agreement binding on the United States, by the Secretary of State.”¹⁸⁹ Current regulations of the various agencies conducting activities in the Arctic acknowledge Executive Order 12114, and all agencies but NOAA seem to indicate an intent to follow its mandate when outside the United States territorial sea.¹⁹⁰ NOAA instead sets out a policy that indicates it will adhere to NEPA instead of the Executive Order 12114 analysis beyond U.S. territory by stating that “NOAA’s policy has been, and continues to be, that the scope of its analysis will be to consider the impacts of actions on the marine environment both within and beyond the U.S. Exclusive Economic Zone (EEZ).”¹⁹¹ Thus, not all federal agencies seem to be following the same policy all the time.

B. ESA Application: Territorial Sea and High Seas

Often undertaken in conjunction with NEPA analysis, consultation for the ESA under Section 7 requires that federal agencies consult with the expert agency (U.S. Fish and Wildlife Service or National Marine Fisheries Service) to “insure that any [agency] action authorized, funded, or carried out by such agency . . . is not likely to jeopardize the continued existence of any endangered species or threatened species . . . [and not destroy or adversely modify its critical habitat.]”¹⁹² Upon consultation, if the activities will affect endangered or threatened species, the expert agency will prepare a biological opinion to determine whether the federal activity would unlawfully jeopardize the species or result in “destruction or adverse modification of critical habitat” of such species.¹⁹³ Moreover, federal agencies (as well as private citizens) are subject to the ESA’s criminal and civil “take” provisions under Section 9, which include prohibiting the taking of endangered or threatened species within the territory of

¹⁸⁹ *Id.*

¹⁹⁰ See NOAA Administrative Order Series 216-6, Environmental Review Procedures for Implementing the National Environmental Policy Act (May 20, 1999); DOD Directive 6050.7, Environmental Effects Abroad of Major Department of Defense Actions (Mar. 31, 1979); Department of Transportation Order 5610.1C, Procedures for Considering Environmental Impacts (Sept. 18, 1979); U.S. DEP’T OF TRANSP., COMMANDANT INSTR. M16475.1D, NATIONAL ENVIRONMENTAL POLICY ACT IMPLEMENTING PROCEDURES AND POLICY FOR CONSIDERING ENVIRONMENTAL IMPACTS (29 Nov. 2000).

¹⁹¹ See NOAA Administrative Order Series 216-6, *supra* note 190.

¹⁹² 16 U.S.C.A. § 1536(a)(2).

¹⁹³ *Id.* § 1536(a)-(b).

the United States, “or the territorial sea of the United States,” or “upon the high seas.”¹⁹⁴ However, the expert agency can provide for incidental taking of a species through an incidental take statement within the biological opinion so long as there is no jeopardy or destruction or adverse modification of critical habitat.¹⁹⁵

The Section 7 consultation provisions within ESA indicate that Section 7 applies to “agency action” but says nothing more as to the reach of the consultation process to activities within certain geographical areas. FWS and NMFS have sought to interpret the statute to require consultation for agency action beyond the United States to the high seas and foreign countries in the past.¹⁹⁶ However, in 1986, after the 1978 Amendments to the ESA, FWS and NMFS promulgated a rule that cut back on the scope of ESA Section 7 consultation to agency action within the “United States, its territorial seas, and the outer continental shelf, because of the apparent domestic orientation of the consultation and exemption processes resulting [from the 1978 amendments] and because of the potential interference with the sovereignty of foreign nations.”¹⁹⁷ While already recognized by 1986, the U.S. EEZ was not mentioned in the joint regulations.¹⁹⁸ In addition, because ESA Section 9(a)(1)(C) prohibits the taking of endangered and threatened species on the high seas by “persons subject to the jurisdiction of the United States,” the joint regulation implied jurisdiction to require consultation under Section 7 for activities within the high seas. The agencies justified this interpretation by reasoning that Congress likely had “concern that compliance with a section 7 incidental take statement not result in a taking violation under section 9(a)(1)(C), as provided in section 7(o)(2).”¹⁹⁹ FWS and NMFS presently continue this policy to require consultation within the high seas.²⁰⁰ The statute and the joint regulations are silent on defining terms such as “territorial sea of the United States” or “high seas” for ESA Section 9 take prohibitions. They are also silent on whether or not foreign EEZs or foreign territorial sea should be part of “high seas” for

¹⁹⁴ *Id.* § 1538(a)(1)(B) & (C).

¹⁹⁵ *See id.* § 1536(b)(4).

¹⁹⁶ *See* Department of Interior and Department of Commerce, Interagency Cooperation, Endangered Species Act of 1973, 43 Fed. Reg. 870, 874 (Jan. 4, 1978).

¹⁹⁷ Department of Interior and Department of Commerce, Interagency Cooperation, Endangered Species Act of 1973—As Amended Final Rule, 51 Fed. Reg. 19,926, 19,929 (June 3, 1986).

¹⁹⁸ *See* Proclamation No. 5030, 48 Fed. Reg. 10,605 (1983).

¹⁹⁹ 51 Fed. Reg., at 19929-30.

²⁰⁰ This rule was challenged in *Defenders of Wildlife v. Hodel*, 658 F. Supp. 43 (D. Minn. 1987). However, ultimately the Supreme Court did not invalidate this rule limiting application extraterritorially and decided instead that the plaintiffs lacked standing. *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992); *see also id.* at 587-89 (Stevens, J., concurring in judgment). Current regulations define “action” as “all activities . . . in the United States or upon the high seas.” 50 C.F.R. § 402.02 (2008).

purposes of the ESA. But Supreme Court precedent that recommends looking to the natural and ordinary meaning of a statute's words, and the presumption against extraterritoriality, cut against the agencies' analysis. These authorities provide justification that "high seas" under the statute should not include foreign EEZs and that it should be "defined by international law as an area free from exercise of foreign sovereign rights over natural resources."²⁰¹ The ESA also allows for listing of species as endangered or threatened that are located outside the United States.²⁰² Together, NMFS and FWS have interpreted the statute to *not* allow for designation of critical habitat "within foreign countries or in other areas outside of United States jurisdiction"²⁰³ because "United States jurisdiction" remains undefined under the ESA and the joint regulations. Nevertheless, NMFS has noted that "United States jurisdiction" for critical habitat designation purposes includes the U.S. EEZ.²⁰⁴ Therefore, at-sea activities currently can expect to enter into consultation under ESA when their actions have exceeded the "may affect" threshold and take place within U.S. territorial seas and high seas and perhaps in the U.S. EEZ.

C. MMPA: U.S. Territorial Sea, U.S. EEZ, and High Seas

The Marine Mammal Protection Act was enacted to protect and conserve marine mammals from human activities. The MMPA prohibits the unauthorized taking of any marine mammal and the import of marine mammals or marine mammal products if the Secretary has determined that the marine mammal should be designated as "depleted."²⁰⁵ The MMPA makes it unlawful for "any person subject to the jurisdiction of the United States" to take a marine mammal on the high seas absent authorization.²⁰⁶ The Act also makes it unlawful "for any person or vessel or conveyance to take a marine mammal in waters or on lands under jurisdiction of the United States."²⁰⁷ Under the Act, "take" encompasses a broad spectrum of actions such as "to harass, hunt, capture, or kill, or attempt to harass, hunt, capture or kill any marine mammal."²⁰⁸ Despite the take prohibition, activities such as scientific research, photography for education and commercial purposes, enhancement of the survival or recovery of a stock, and other non-commercial fishing activities that have only a negligible impact on the

²⁰¹ Gibel, *supra* note 28, at 47.

²⁰² See 16 U.S.C.A. § 1533(b).

²⁰³ 50 C.F.R. § 424.12(h) (2008).

²⁰⁴ Department of Commerce, Designated Critical Habitat, Northern Right Whale, Final Rule, 59 Fed. Reg. 28,793, 28,801 (June 3, 1994).

²⁰⁵ 16 U.S.C.A. § 1371(a).

²⁰⁶ *Id.* § 1372(1).

²⁰⁷ *Id.* § 1372(2)(A).

²⁰⁸ *Id.* § 1362 (13).

species or stock may be issued an incidental take permit for one to five years.²⁰⁹ The MMPA specifically defines “waters under the jurisdiction of the United States” to include “territorial sea of the United States . . . , the contiguous [zone] to the territorial sea [out to] 200 nautical miles from the baseline from which the territorial sea is drawn,” and “the areas referred to as eastern special areas in Article 3(1) of the Agreement between the United States of America and [Russia] on the Maritime Boundary, signed June 1, 1990.”²¹⁰

Interestingly, while the statute clearly prohibits takes on the high seas or within waters of the United States, it is silent on whether the take prohibition or permitting requirements for U.S. citizens apply in a foreign EEZ or foreign territorial sea. However, this has not dissuaded NMFS from requiring U.S. citizens to apply for an MMPA permit within foreign EEZs. Just recently, NMFS stated this policy in a proposed rule to issue an incidental take authorization to a U.S. research organization that was planning to conduct a seismic survey in Southeast Asia. In noting that the proposed action was planned to traverse not only the high seas, but also the territorial seas and the EEZ of the foreign nation, NMFS noted that it “does not authorize the incidental take of marine mammals in the territorial seas of foreign nations as the MMPA does not apply in those waters.”²¹¹ It appears that NMFS views MMPA jurisdiction in a foreign EEZ but not the territorial sea of a foreign nation just as if that water space is part of the high seas—where MMPA applies and where every nation may assert jurisdiction over its own nationals and each nation has a duty to cooperate regarding conservation and management of marine resources. NMFS makes no statement of the distinctions that are well understood regarding how the geographic areas are defined under UNCLOS. Even prior to this proposed rulemaking, NMFS opined that a Foreign EEZ is part of the “high seas” in an interagency letter by its General Counsel provided to the Department of Justice in 2003.²¹² This opinion is noted in NMFS regulations that require MMPA take permits by anyone subject to U.S. jurisdiction outside of the territorial sea and high seas because NMFS interprets the general moratorium provision as an additional prohibition of taking, although the moratorium on takings is not listed

²⁰⁹ See *id.* § 1371(a)(3)(B), 1371(a)(5)(A) & (D).

²¹⁰ *Id.* § 1362 (15).

²¹¹ NOAA, “Proposed Incidental Take Authorization: Incidental Takes of Marine Mammals During Specified Activities; Marine Geophysical Survey in Southeast Asia March-July 2009,” 73 Fed. Reg. 78294 (Dec. 22, 2008). NOAA, “Incidental Takes of Marine Mammals During Specified Activities; Marine Geophysical Survey in the Northeast Pacific Ocean, August – October, 2009,” 74 Fed. Reg. 42861, 42862 (Aug. 25, 2009).

²¹² See Gibel, *supra* note 28, at 44 & nn.126 & 159 (noting that under *Chevron* or even *Skidmore* analysis, NOAA’s opinion, expressed in a letter and in other informal ways through the years that a foreign EEZ is part of the high seas and thus should allow for MMPA regulation in the EEZ, is likely lacking power to persuade to be entitled to deference by a court).

in MMPA Section 1372 as a category of the prohibited acts; rather, it is separately noted in Section 1371.²¹³ In fact, NMFS has also recently issued a permit for the incidental take of marine mammals during a marine seismic survey within the Canadian EEZ in the northeast Pacific Ocean.²¹⁴ But the preamble of the notice lacks any justification for requiring the permit. Rather, the notice presumes authority within the Canadian EEZ. This is evident from a response to a comment in the notice about whether Canada has been consulted and commented on the proposed activity.²¹⁵ The response does not indicate whether NMFS provided the Canadian government with the application for the proposed activity but only notes that “NMFS received no comments from the Canadian government or from any Canadian organization during the public comment period.”²¹⁶ But NMFS indicates that the National Science Foundation is “encouraged to coordinate with the Canadian government regarding the proposed seismic activity.”²¹⁷ It is evident that NMFS is continuing to advance its position that the foreign EEZ is part of the high seas for MMPA permitting.²¹⁸ Thus far, that opinion has advanced with no opposition. However, it has *not* been deferred to by any court ruling to extend MMPA applicability to U.S. activities within foreign EEZs.

But there is some case law on the scope of the MMPA. The Fifth Circuit Court of Appeals in *United States v. Mitchell* determined that the MMPA take prohibition does not extend beyond the high seas to territory (including territorial waters) of a foreign sovereign.²¹⁹ That court found that the MMPA and its legislative history do not express clear intent to overcome the presumption against extraterritorial application of U.S. laws. The court viewed MMPA as a conservation statute that has force to the extent that “the United States has [control] over the natural resources within its territory.”²²⁰ And when passed into law, Congress “presumably recognizes the authority of other sovereigns to protect and exploit their own resources. Other states may strike

²¹³ See 16 U.S.C.A. § 1371, 1372; 50 C.F.R. § 216.11(c) (2008).

²¹⁴ See NOAA, Incidental Takes of Marine Mammals During Specified Activities; Marine Geophysical Survey in the Northeast Pacific Ocean, August—October, 2009, 74 Fed. Reg. 42,861, 42,864 (Aug. 25, 2009).

²¹⁵ See *id.* at 42,864.

²¹⁶ *Id.*

²¹⁷ *Id.*

²¹⁸ This interpretation by NMFS begs the concerning question of whether a foreign nation, perhaps without the same protections for the environment as those embodied in the MMPA, could establish permitting authority under a law to issue its citizens permits for activities within the United States EEZ.

²¹⁹ *United States v. Mitchell*, 553 F.2d 996, 1005 (5th Cir. 1977); see also Gibel, *supra* note 28, at 46-48.

²²⁰ 553 F.2d at 1002.

balances of interests that differ substantially from those struck by Congress.”²²¹ The court recognized that the international nature of resolving differences is through collaboration or negotiation rather than “through the imposition of one particular choice by a state imposing its law extraterritorially.”²²² The language of the MMPA also requires that the Department of State seek international marine mammal protection through use of negotiation, treaty, and convention, which gives more indication that the MMPA was not intended to apply beyond U.S. territorial waters or the high seas.²²³ The *Mitchell* court, in its review of the legislative history of the MMPA, noted that while the moratorium in Section 1371 and the taking prohibitions in Section 1372 appear inter-related in the statute, a committee report prior to enactment failed to explain the need of both provisions but did indicate that there could be instances where the moratorium would not apply and therefore no permit would need to be issued such as when international agreements, like the North Pacific Fur Seal Convention, existed.²²⁴ Therefore, the court indicated that it was unclear whether “the moratorium was intended to have broader territorial effect than the prohibitions, which do not reach conduct in the territory of other sovereigns.”²²⁵

In 1996, after the MMPA was amended in 1994 to establish an expedited process to authorize harassment of small numbers of marine mammals incidental to lawful activities, NOAA proposed and eventually promulgated new regulations on incidental take of marine mammals specifically in the Arctic. These regulations define “Arctic waters” as “marine and estuarine waters north of 60° N” latitude.²²⁶ This definition seems to hold no limits as to where in “Arctic waters” a U.S. citizen will be required to have an incidental harassment authorization for certain activities, including all the way up to 90° N latitude at the North Pole regardless of sovereign claims and rights of other nations.²²⁷ Other than the proposed permit within the Canadian EEZ, thus far there appear to be no permits issued in other nations’ EEZs or territorial seas in the Arctic Ocean.

²²¹ *Id.*

²²² *Id.* at 1002-1003.

²²³ *See id.* at 1004.

²²⁴ *Id.* at 1001.

²²⁵ *Mitchell*, 553 F.2d at 1001.

²²⁶ 50 C.F.R. § 216.103 (2008).

²²⁷ If one reads the definition in the most literal and expansive reading, it would include all waters lying partly or wholly above that 60°N latitude.

VI. LIMITS OF APPLICATION OF THE U.S. LAWS TO FUTURE ARCTIC
MARITIME ACTIVITIES

The outcomes of the existing disputes between the United States and other nations in the Arctic seas could play a significant role in determining whether federal agencies should apply NEPA or the Executive Order 12114 requirements, MMPA, and ESA in certain areas. For instance, depending on how the disputed ocean area in the Beaufort sea is settled, it could become U.S. territorial sea and EEZ, or it could become Canadian territorial sea and EEZ. Should the United States gain that portion in its entirety or some part of it, an environmental planner would have to ensure the NEPA or Executive Order 12114 analysis and ESA consultation are done and MMPA take authorization is received before an activity can commence in the U.S. territorial sea portion or U.S. EEZ. In the high seas areas of the Arctic, MMPA and ESA application would be required (assuming threshold requirements are triggered) with Executive Order 12114 instead of NEPA analysis. And activities within any portion beyond the territorial sea out to the limit of the U.S. EEZ or in a foreign EEZ would require analysis “in further[ance] [of] the purpose of [NEPA]” under Executive Order 12114.²²⁸

But as activities in the Arctic start to become more common and likely more scrutinized by environmental watchdog groups, the arguments for and against extraterritorial application may be more relevant. The Arctic could be where these undecided application issues get pushed to the forefront.

A. NEPA

Based on existing case law and policy, NEPA has at times been applied to activities outside of the territory of the United States. When courts have expressed desire to extend NEPA extraterritorially, they have chosen not to extend it when it may interrupt foreign relations or long-standing treaty relationships.²²⁹ The *Massey* court, upon deciding to apply NEPA to Antarctica, specifically noted that it was not deciding “how NEPA might apply to actions in cases involving an actual foreign sovereign.”²³⁰ Depending on the location in the Arctic Ocean, a federal activity having significant impact on the environment could be having an effect on foreign policy and relations of the United States with one Arctic nation or the entire Arctic Council. Arctic neighbors who are resolving their maritime claims could have concerns over their sovereignty

²²⁸ Executive Order 12114, Environmental Effects Abroad of Major Federal Actions, 44 Fed. Reg. 1957 (Jan. 4, 1979).

²²⁹ See *supra* notes 139-184 and accompanying text.

²³⁰ *Envtl. Def. Fund v. Massey*, 986 F.2d 528, 537 (D.C. Cir. 1993).

being violated if U.S. agencies undertake NEPA analysis in a manner that does not include proper consideration of that nation's laws, jurisdiction, and public participation in the process. The United States clearly does not have legislative control or sovereignty in the EEZ of another country to apply its law within that foreign EEZ. Executive Order 12114, however, provides for NEPA-like analysis with some nuanced differences to keep the interests of other nations in mind. For instance, the analysis under Executive Order 12114 defines the "environment" in a way that considers "natural and physical environment and excludes social, economic and other environments," and requires State Department coordination with foreign governments concerning the communications between a U.S. agency and any foreign government.²³¹ Executive Order 12114 also allows for some specific activity exemptions from the analysis required. The exemptions include non-significant actions outside the United States, actions by or "pursuant to the direction of the President" when national security is involved, actions relating to intelligence and arms transfers, actions during armed conflict, or actions pertaining to disaster and emergency relief, as well as other actions.²³² Moreover, the Executive Order allows for flexibility through modification as necessary in "content, timing and availability of documents to other affected federal agencies and affected nations" for various reasons, such as ensuring appropriate consideration of diplomacy, national security, governmental or commercial confidentiality, ability for an agency to act promptly and to "avoid adverse impacts on foreign relations or infringement in fact or appearance of other nation's sovereign responsibilities."²³³ Therefore, it may be best to leave current interpretation and policy over NEPA's coverage to the territorial sea limits and follow the procedures of Executive Order 12114 further out to sea.

NEPA should not be applied outside the territory of the United States because CEQ, the agency charged to administer NEPA, has not promulgated a valid and binding opinion on extraterritoriality. Since the CEQ has never promulgated a regulation saying NEPA applies extraterritorially, there is no opinion to which agencies and courts can defer. While Executive Order 12114 exists, it calls for a slightly different analysis, but appears on its face to be a strong indication of an attempt to resolve the dispute as to extraterritorial acts. Executive Order 12114 states that it "represents the United States government's exclusive and complete determination of procedural and other actions to be taken by Federal agencies to further the purpose of [NEPA]," outside of the United States.²³⁴ Courts have routinely given great deference to agencies

²³¹ 44 Fed. Reg. 1957.

²³² *Id.*

²³³ *Id.*

²³⁴ *Id.*

interpreting executive orders charged to their administration.²³⁵ But, if the agency is not in charge of administering the executive order, there is less clarity on whether deference should be afforded to that agency. At least one court has suggested no deference is afforded.²³⁶ The Supreme Court has found that CEQ's interpretation of NEPA through regulations should be given substantial deference,²³⁷ but no court has determined that another federal agency interpreting the Executive Order 12114 should be given substantial deference.²³⁸

Nevertheless, the presumption against extraterritoriality is applicable to NEPA when outside of the territorial sea of the United States. While the Supreme Court has stated that federal statutes apply to areas where the United States has sovereignty or "has some measure of legislative control,"²³⁹ taking that statement to its ultimate conclusion would turn the U.S. EEZ, where the United States has "some" legislative control over natural resources, into an extension of the U.S. territory, thereby presumptively applying all federal laws there. But this is against the Supreme Court's pronouncement that statutes presumptively apply "only within the territorial jurisdiction of the United States."²⁴⁰ According to customary international law, as now noted in UNCLOS, the U.S. EEZ falls outside of U.S. territory (as any coastal nation's EEZ falls outside its own territorial sea);²⁴¹ therefore, federal legislation is presumed to be inapplicable in it.²⁴² Also, because the presumed intent of Congress is to legislate with a focus on "domestic concerns," one could argue that it is difficult to assume that Congress intended more often than not for federal legislation to apply to large expanses of the ocean space in the Atlantic, Pacific or the Arctic Oceans.²⁴³ If "some" degree of legislative control is the amount needed to

²³⁵ See *Udall v. Tallman*, 380 U.S. 1, 16-18 (1965); see also *Kester v. Campbell*, 652 F.2d, 13 (9th Cir. 1981);

²³⁶ *American Federation of Government Employees, AFL-CIO, Council 147 v. Federal Labor Relations Authority* 204 F.3d 1272, 1275 (9th Cir. 2000) (indicating that de novo review is reasonable for when an agency is interpreting an executive order that it is not charged with administering).

²³⁷ See *Andrus v. Sierra Club*, 442 U.S. 347 (1979); see also *Klick*, *supra* note 28, at 301 & n.81.

²³⁸ This is due to the issue being seldom argued since the Executive Order does not allow for a private cause of action. See Executive Order 12114, Environmental Effects Abroad of Major Federal Actions, 44 Fed. Reg. 1957, (Jan. 4, 1979).

²³⁹ *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991).

²⁴⁰ *Id.* (quoting *Foley Bros. Inc. v. Filardo*, 336 U.S. 281, 285 (1949)) (emphasis added).

²⁴¹ See UNCLOS, *supra* note 6, arts. 55 & 62-68 (defining EEZ as "beyond and adjacent to the territorial sea" and setting the parameters of the coastal state's jurisdiction over conservation and management of various species).

²⁴² See generally *Argentine Republic v. Armerada Hess Shipping Corp.*, 488 U.S. 428, 440-41 (1989) (noting that federal laws do not apply beyond U.S. territorial waters absent an expression of congressional intent otherwise). "When it desires to do so, Congress knows how to place the high seas within the jurisdictional reach of a statute." *Id.* at 440.

²⁴³ See generally *Smith v. United States*, 507 U.S. 197, 204 (1993).

nullify the presumption against extraterritoriality, rather than the express congressional intent, then practically no area would be off limits to U.S. federal law, including international waters, the global commons and even foreign nations (regarding any U.S. citizens present in that nation). There would be little that remains of the presumption. Though one district court has decided that NEPA should apply within the United States EEZ, despite a lack of clear intent by Congress to state such a proposition in the statute, other courts have held that the laws of the United States as they pertain to “trust territories” of the United States, which fall outside of the definition of “U.S. territory” are never presumed to apply unless they are specifically made applicable by Congress.²⁴⁴ Typically, Congress has more exclusive legislative control over trust territories than its limited authority in the U.S. EEZ for the purpose of conserving and managing natural resources.²⁴⁵ Therefore, absent express congressional intent, the presumption against extraterritoriality should not be overcome to apply NEPA in the U.S. EEZ and beyond.

On the other hand, proponents for applying NEPA essentially anywhere in the Arctic will likely argue that the presumption against extraterritoriality is overcome or simply does not apply to NEPA. This argument hinges on viewing the intent of Congress in writing NEPA to apply it in a far-reaching way to the “human environment” and to “encourage productive and enjoyable harmony between man and his environment; [and] to promote efforts which will prevent or eliminate damage to the environment and biosphere”²⁴⁶ By this language, and the Section 102 language directing agencies to carry out NEPA “to the fullest extent practicable,” it is argued that Congress had express intent to apply NEPA outside of the United States.²⁴⁷ Secondly, even if this language does not amount to express intent in the law, still the legislative history demonstrates that global impacts and impact in other countries were intended to be within the scope of NEPA’s EIS requirement. Statements regarding the worldwide context are arguably found in various Joint, House and Senate Reports as well as verbal comments, especially those made by Senator Henry

²⁴⁴ See *Gushi Bros. Co. v. Bank of Guam*, 28 F.3d 1535, 1540-43 (9th Cir. 1994); see also *Gale v. Andrus*, 643 F.2d 826, 834 (D.C. Cir. 1980).

²⁴⁵ See *Gushi Bros.*, 28 F.3d at 1540 (“Article 3 of the Trusteeship Agreement provided, in pertinent part, that the United States ‘may apply to the trust territory . . . such of the laws of the United States as it may deem appropriate to local conditions and requirements.’ Trusteeship Agreement, art. 3 (quoted in *Porter*, 496 F.2d at 587). The Trust Territory Code, promulgated pursuant to the Agreement, provided only that American common law was to apply to the Trust Territory during the period of United States administration. 1 Trust Territory Code § 103 (1980).”).

²⁴⁶ 42 U.S.C.A. § 4321 (West 2009).

²⁴⁷ 42 U.S.C.A. § 4332 (West 2009); see also Russell W. Peterson, CEQ Chairman, Memorandum on the Application of the EIS Requirement to Environmental Impacts Abroad of Major Federal Actions, September 24, 1976, 42 Fed. Reg. 61,068 (Dec. 1, 1977); see also Klick, *supra* note 28, at 298-99.

Jackson, the NEPA bill's sponsor.²⁴⁸ But previous courts have found that NEPA's legislative history does not support rebutting the presumption since it does not show clear and unambiguous intent by Congress.²⁴⁹ In fact, NEPA lacks reference to foreign nations or international considerations except for Section 102(2)(F), which directs all agencies to, "where consistent with foreign policy of the United States, lend appropriate support . . . to maximize international cooperation" to protect the environment.²⁵⁰ But even this does not clearly indicate NEPA applies outside of the U.S. territorial sea; rather, it indicates merely that agencies should seek to cooperate internationally on environmental issues when outside of U.S. territory, just as the United States is doing through the Arctic Council initiatives already.

With the spotlight on the Arctic, it is fair to anticipate that any at-sea activity in the Arctic will face potential public scrutiny of greater proportion. There will likely be more challenges to any assessment short of an EIS, given the reality of the Arctic's heightened sensitivity throughout its ecosystems. If an agency is applying NEPA, then it is likely that the potential for litigation on the adequacy of that analysis will increase. As a defense to not doing analysis in certain maritime zones such as the EEZ, the high seas or even a foreign EEZ, an agency may choose to argue the issue of extraterritoriality and raise the presumption against it. But that decision will depend upon an individual agency's perspective on NEPA coverage, so the issue may not arise.²⁵¹ Even though Executive Order 12114 analysis bars judicial review, with NEPA's extraterritorial application still undecided, litigants might press for the Arctic to be viewed through the eyes of the *Massey* court, as allowing for NEPA coverage throughout the Arctic based upon "some legislative control" that the United States does have over the area such as in the U.S. EEZ and possibly in the high

²⁴⁸ See 42 Fed. Reg. 61,068 (noting Senator Jackson's comments during floor debates over NEPA indicated that through NEPA Congress was intending to avoid danger to mankind, and also noting post-enactment history of the House Merchant Marine and Fisheries Committee's view that global effects are relevant to the decision-making process and must be considered); see also Klick, *supra* note 28, at 298-99.

²⁴⁹ See *Natural Res. Def. Council v. Nuclear Regulatory Comm'n*, 647 F.2d 1345, 1367 (D.C. Cir. 1981) (noting that the intention of the Congress which ultimately enacted NEPA was unclear). The court in this case concluded "that NEPA's legislative history illuminates nothing in regard to extraterritorial application." *Id.*

²⁵⁰ 42 U.S.C.A. § 4332(F) (West 2009).

²⁵¹ Given NOAA's policy for NEPA implementation, it is likely that NOAA would not urge the argument to be made as a defense, since its activities generally include development of fishery management plans and regulations, authorization of the take of protected species and marine mammals incidental to fishing and other activities, and conducting and authorizing scientific research. See NOAA Administrative Order Series 216-6, Environmental Review Procedures for Implementing the National Environmental Policy Act (May 20, 1999).

seas.²⁵² A litigant may argue that the United States has similarly some “legislative control” over such things as air transportation and search and rescue operations. But in reality, that control is different from the control in Antarctica and is more likely shared (or on the verge of being shared) in some multilateral way among the Arctic nations because of the efforts of the Arctic Council in collaborating on environmental protection and safety measures.²⁵³ Some argue that *Massey*’s reasoning to require NEPA in all areas of the Arctic Ocean expanse will not hamper U.S. foreign policy or prove incompatible with Section 102(2)(F)’s mandate to lend support to international cooperation that is consistent with the foreign policy of the United States.²⁵⁴ However, since there are foreign sovereign interests within the maritime spaces in the Arctic that are seemingly set on maintaining sovereign control of respective areas, that justification from *Massey* should not control.

Short of final resolution of the question of NEPA’s extraterritorial application, a delicate balance in the application of domestic law must be achieved given existing international policy in the Arctic. For instance, in 1997 in the Alta Declaration, the member nations of the Arctic Council adopted a set of guidelines for environmental impact assessment (“EIA”) in the Arctic.²⁵⁵ These guidelines do not carry the force of law but in the Alta Declaration, the nation states of the Arctic Council (including the United States) agreed to accept and apply them.²⁵⁶ Primarily, the guidelines “aim at providing suggestions and examples of good practice to enhance the quality of Environmental Impact Assessments²⁵⁷ and the harmonization of EIA in different parts of the Arctic.”²⁵⁸ The guidelines call for specific Arctic thresholds to trigger an EIA and also note that “national laws do not always take into account the sensitivity of arctic areas, which may require lower threshold levels.”²⁵⁹ Noticeably different from NEPA or Executive Order 12114 analyses, the guidelines call for encouragement of the use of the precautionary approach in the Arctic, since “baseline data [is] scarce

²⁵² *Env’tl. Def. Fund v. Massey*, 986 F.2d 528, 533-36 (D.C. Cir. 1993).

²⁵³ ARCTIC COUNCIL, *supra* note 58, at 6 (calling for a multi-lateral search-and-rescue agreement among the nations of the Arctic and calling Arctic nations to look at their shipping regulatory regimes and explore harmonizing those regimes with uniform Arctic safety and environmental protection regimes, consistent with UNCLOS).

²⁵⁴ *Massey*, 986 F.2d at 533-36.

²⁵⁵ Arctic Environmental Protection Strategy, Guidelines For Environmental Impact Assessment (“EIA”) in the Arctic, <http://arcticcentre.ulapland.fi/aria/index.asp> (last visited Oct. 9, 2009). *See also* The Alta Declaration, <http://arctic-council.org/filearchive/The%20Alta%20Declaration.pdf> (last visited Oct. 9, 2009).

²⁵⁶ The Alta Declaration, *supra* note 255.

²⁵⁷ EIA is a generic term that includes the term “Environmental Impact Statements” as known under U.S. law.

²⁵⁸ Arctic Environmental Protection Strategy, *supra* note 255.

²⁵⁹ *Id.* at 11-12.

and there are gaps in the understanding of the important ecological functions in the Arctic systems.”²⁶⁰ But there are common requirements, such as alternatives analysis and public participation, that are encouraged early and often throughout the process of conducting an EIA within the Arctic.²⁶¹ The public participation is to include the involvement of the indigenous people of the Arctic who hold “special knowledge of the Arctic.”²⁶² While NEPA has not been amended to provide for conformity with these guidelines specifically assessing Arctic activities, federal planners should ensure that any NEPA or Executive Order 12114 analysis considers the fundamental differences of the Arctic highlighted in the guidelines. The unique nature of the Arctic, especially when preparing for the public participation element and consideration of indigenous community concerns and mitigation measures to minimize conflicts and alleviate environmental impacts, should be taken into account. Every effort should be made in agency planning to ensure that decisions take into account risks and “proceed on the basis of best available information” despite limitations on existing baseline data about the state of the Arctic Ocean ecosystem.²⁶³ Keeping with the status quo—where NEPA is applied only within the territory of the United States and Executive Order 12114 coverage is outside of that territory—should not mean there is less environmental analysis by agencies. In fact, sometimes activities in the marine environment are not stationary, so it is likely there will be impact within more than one maritime zone to require application of both NEPA and Executive Order 12114. But when major federal actions are wholly within one maritime zone outside of the territorial sea of the United States, applying the presumption will simply mean that Executive Order 12114 applies, which in comparison to NEPA allows more respect for sovereignty of other nations, more coordination among the foreign governments as needed, flexible modification of the timing and content of prepared documents, and more consideration of diplomatic and national security concerns.²⁶⁴

B. ESA

When boundary disputes are resolved in the Arctic, ESA compliance by agencies also will require at minimum consultation on activities meeting the “may affect” threshold within the U.S. territorial sea including the high seas (if an incidental take statement may be needed). The status of the U.S. EEZ is still debatable since the joint regulations for Section 7 consultation fail to make

²⁶⁰ *Id.* at 10.

²⁶¹ *See id.* at 14-15.

²⁶² *Id.* at 15.

²⁶³ Directive on Arctic Region Policy, *supra* note 4.

²⁶⁴ *See* Executive Order 12114, “Environmental Effects Abroad of Major Federal Actions,” 44 Fed. Reg. 1957 (Jan. 4, 1979).

mention of the area. An ordinary meaning of the area often indicates that it is an area “just beyond the territorial sea.”²⁶⁵ Although a NEPA-related decision on extraterritoriality to the U.S. EEZ was made in *NRDC v. Navy*, the court’s determination was based on the “legislative control” that the United States has over the area, so it is likely that ESA justifiably applies in the U.S. EEZ.²⁶⁶ However, agencies engaged in maritime activities should not have to consult or have an incidental take statement regardless of triggering the “may effect” threshold for activities within another country’s EEZ, territorial sea, and possibly extended continental shelf. To apply the ESA to activities within those areas that are subject to another’s sovereignty and jurisdiction may cause interference with the foreign relationships already well established between the Arctic nations through application of the UNCLOS and Arctic Council initiatives.²⁶⁷ Presently, FWS has not altered or expanded its interpretation of where critical habitat can be designated, as seen through its recent proposed designation of critical habitat for the iconic symbol of the Arctic, the polar bear.²⁶⁸ FWS decided to continue not to designate critical habitat beyond U.S. territorial sea and U.S. waters when it chose to propose regulations identifying critical habitat for the polar bear of 200,541 square miles “located in Alaska and adjacent territorial and U.S. waters.”²⁶⁹ Nevertheless, the creation of critical habitat means that agencies with proposed actions that may adversely modify or destroy the critical habitat must consult prior to those projects being undertaken.

The interpretation of Section 7 of the ESA to require consultation extraterritorially by FWS and NMFS in the joint regulations continues to be debatable. It is certainly evident that ESA Section 7(a)(2) lacks language regarding its scope. This supports the argument that the ESA Section 7 consultation does not show a clear and unambiguous statement of congressional intent required by the Supreme Court to rebut the presumption against extraterritoriality.²⁷⁰ The resource agencies claim that by cross-reference to the take provision in ESA Section 9 within Section 7(o)(2), there is intent by

²⁶⁵ BLACK’S LAW DICTIONARY 587 (7th ed. 1999); *see also* UNCLOS, *supra* note 6, art. 55.

²⁶⁶ *NRDC v. Navy*, 2002 U.S. Dist. LEXIS 26360 *1, *41-42 (C.D. Cal. 2002).

²⁶⁷ Under Article 193 of UNCLOS, states have sovereign rights to exploit their natural resources pursuant to their environmental policies and there is a general obligation to protect and preserve the marine environment under Article 192 as well as to cooperate both globally and regionally for protection and preservation of the marine environment under Article 197. *See* UNCLOS, *supra* note 6, arts. 192, 193 & 197.

²⁶⁸ Department of Interior, U.S. Fish and Wildlife, “Endangered and Threatened Wildlife and Plants; Designation of Critical Habitat for the Polar Bear (*Ursus maritimus*) in the United States, Proposed Rule,” 74 Fed. Reg. 208 (Oct. 20, 2009). A rule finalizing the designation is due by FWS before the court ordered deadline of June 30, 2010. *See id.*

²⁶⁹ *Id.*

²⁷⁰ *See supra* notes 200-204 and accompanying text.

Congress to have the consultation provision apply beyond United States territory.²⁷¹ The pertinent language in Section 7(o)(2) reads:

Notwithstanding sections . . . 1538(a)(1)(B) and (C) [Section 9(a)(1)(B) and (C)] of this act, sections 1371 and 1372 of this title [the Marine Mammal Protection Act of 1972], or any regulation promulgated to implement any such section— . . . (2) any taking that is in compliance with the terms and conditions specified in a written statement provided under subsection (b)(4)(iv) of this section [Section 7 consultation] shall not be considered to be a prohibited taking of the species concerned.²⁷²

The provision appears to allow a mechanism to exempt from take provisions so long as there is compliance with “terms and conditions” developed into the biological opinion.²⁷³ But this link of the consultation provision to the “high seas” term in the take provision under Section 9 of the ESA is subject at best to varying interpretation. Congress may have been merely exercising caution by noting that any “take” that occurs after a consultation is completed would be deemed legal. Or Congress could have included the Section 9(a)(1)(C) reference to ensure that agency actions within U.S. territorial seas having an adverse effect on endangered species on the high seas have a permit. In a court, the regulation could receive deference, although it is likely to never be the subject of litigation.²⁷⁴ But regardless of possible interpretations, any court faced with determining if ESA Section 7 applies beyond U.S. territory will not be required to “choose between . . . competing interpretations” since the presumption against extraterritoriality requires the court to look only to “affirmative intention . . . clearly expressed.”²⁷⁵ And, even within the joint

²⁷¹ Department of Interior and Department of Commerce, Interagency Cooperation, Endangered Species Act of 1973—As Amended Final Rule, 51 Fed. Reg. 19,926, 19,929-30 (June 3, 1986).

²⁷² 16 U.S.C.A. § 1536(o)(2).

²⁷³ *Id.*

²⁷⁴ See *Chevron v. Natural Res. Def. Council*, 467 U.S. 837 (1984) (indicating that a court will defer to an agency’s reasonable interpretation of an ambiguous statute). However, the question of whether the joint regulation is a reasonable interpretation would never be raised because it would only benefit other governmental agencies rather than a citizen to raise it against FWS and NMFS. Given that there cannot be a lawsuit by one traditional Article II Executive Branch agency against another, this aspect of the regulation will likely never be addressed. See *SEC v. Fed. Labor Relations Auth.*, 568 F.3d 990, 996-97 (D.C. Cir. 2009) (Kavanaugh, J., concurring) (explaining the oddities of two Executive Branch agencies in litigation against each other).

²⁷⁵ *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248, 250 (1991) (citing *Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957)). See also *Litecubes, LLC v. Northern Light Products*, 523 F.3d 1353, 1363 n.9 (Fed. Cir. 2008); *Subafilms, Ltd. V. MGM-Pathe Commc’n Co.*, 24 F.3d 1088, 1095-96 (9th Cir. 1994).

regulation preamble discussing the scope issue, the agencies note that any intent by Congress is not express and only implied at best.²⁷⁶ Therefore, the presumption against extraterritoriality is not rebutted based on the language of ESA. However, even if a court is able to find the presumption rebutted, the term “high seas” must be examined to determine where the outer limits of such application exists. Since arguments regarding how to determine what “high seas” means apply to review of the scope of both the ESA as well as the MMPA, the discussion proceeds below.

C. MMPA

NOAA’s and NMFS’s policy on where the MMPA requires take authorization appears to include areas beyond the geographic boundaries clearly expressed in the statute. As more activities start to take place within the Arctic, whether MMPA take authorizations will be required for United States activities beyond the high seas into a foreign EEZ or foreign territorial sea remains to be seen. And it remains to be seen how such application will disrupt the delicate foreign relationships of the Arctic Council nations. Reliance by NMFS on the general moratorium on take within MMPA to glean intent of Congress to expand the permit requirement to areas beyond the high seas is questionable.²⁷⁷ Because no court has specifically found that the general moratorium language expresses Congress’ unambiguous intent to apply MMPA beyond U.S. territory, the presumption should still apply to limit MMPA.

The regulations requiring incidental small take permits in the broadly-phrased “Arctic waters” have the potential to assume and assert U.S. authorization where the United States has clearly no authorization under the MMPA’s statutory text.²⁷⁸ The MMPA does appear to have some limitation in where it is applied just by looking at the definition of “waters under the jurisdiction of the United States.”²⁷⁹ The statute does indicate clear coverage of territorial seas and the U.S. EEZ, as well as the “eastern special area” negotiated between the United States and Russia as part of the “waters under the jurisdiction of the United States.” Therefore, they are within the scope of MMPA’s take prohibition under Section 1372(a)(2)(A) that applies to any person or vessel (not just U.S. citizens) “in waters or lands under jurisdiction of the United States.”²⁸⁰ Given that definition, coverage under Section 1372(a)(1) then must be read to apply in areas beyond the U.S. territorial sea or EEZ

²⁷⁶ See *supra* notes 200-204 and accompanying text.

²⁷⁷ See *supra* notes 212-213 and accompanying text.

²⁷⁸ See *supra* notes 226-227 and accompanying text.

²⁷⁹ 16 U.S.C.A. § 1362(15).

²⁸⁰ *Id.* § 1362(15), 1372(a)(2)(A). See also *supra* notes 169-174 and accompanying text.

because it is likely that Congress did not intend for a U.S. person to be in violation of both sections for one activity. But whether the statute intended to cover a foreign EEZ is still ambiguous. If the concept of the EEZ is meant to be part of “high seas,” as NMFS seems to indicate in rulemaking preamble language, then in reading the MMPA text there appears no justification for excluding U.S. EEZ, as is done under the definitions section (Section 1362(15)) of the MMPA, and still concluding that foreign nation EEZs are part of the high seas for which coverage is found under Section 1372(a)(1)’s additional restrictions applying to U.S. persons and vessels. Just as the degree of sovereignty that the U.S. exercises over its EEZ is sufficient to remove the U.S. EEZ from “high seas,” so should the degree of sovereignty a foreign nation exercises over its respective EEZ be sufficient to keep foreign EEZs beyond the scope of MMPA. Therefore, it is reasonable to conclude that both the U.S. EEZ and foreign EEZs are not part of the “high seas.” This reasoning is further supported by the fact that when Congress was drafting the MMPA, it chose to reject a definition of high seas recommended by Department of Commerce of “waters seaward of the territorial sea of the United States” that would have been static and fixed.²⁸¹ Additionally, when looking at the ESA, a similar recommendation was not made when that law was being debated.

If Congress intended the term “high seas” always to refer to a specific geographic area regardless of subsequent developments in domestic and international law, it would have added a definition as it has done in other pieces of legislation.²⁸² Otherwise, when Congress uses a term, in the absence of a definition indicating otherwise, it is “presume[d] Congress intended to incorporate the common definition of that term.”²⁸³ By defining a term of art in a specific statute, Congress intends for that definition to be limited only to that statute.²⁸⁴ Therefore, absent a specific defined term of art for “high seas” in either the MMPA or ESA, it is reasonable to conclude that foreign EEZs are excluded from the high seas, since customary international law recognizes that

²⁸¹ Letter from Karl E. Bakke, Acting General Counsel, Department of Commerce, to Edward A. Garmatz, Chairman, House Committee on Merchant Marine and Fisheries (Sept. 10, 1971), *reprinted in* 1972 U.S.C.C.A.N. 4144, 4167, 4170 (1972).

²⁸² *See, e.g.*, Fisheries Conservation and Management Act of 1976, 16 U.S.C.A. § 1802(20) & (50) (West 2009) (defining high seas as “all waters beyond the territorial sea of the United States and beyond any foreign nation’s territorial sea, to the extent that such sea is recognized by the United States” and defining waters of a foreign nation as “any part of the territorial sea or exclusive economic zone (or the equivalent) of a foreign nation, to the extent such territorial sea or exclusive economic zone is recognized by the United States”).

²⁸³ *United States v. Vargas-Amaya*, 389 F.3d 901, 904 (9th Cir. 2004); *see also* *Richards v. United States*, 369 U.S. 1, 9 (1962).

²⁸⁴ *See* *Burgess v. United States*, 128 S. Ct. 1572, 1577 (2008); *Russello v. United States*, 464 U.S. 16, 23 (1983).

each nation is primarily responsible for protecting and preserving natural resources such as marine mammals within its own EEZ.²⁸⁵ The ordinary meaning of a word is often found in a simple dictionary definition. Even *Black's Law Dictionary* indicates that "high seas" traditionally meant "seas or oceans beyond the jurisdiction of any country" and "[u]nder international law, the high seas traditionally began three miles from the coast, but under the [UNCLOS] coastal shores now have a 200-mile exclusive economic zone."²⁸⁶ It appears that the ordinary meaning of "high seas" starts beyond any EEZ. As noted earlier, UNCLOS defines high seas to be those parts of the sea that are "not included in the exclusive economic zone, in the territorial sea or in the internal waters of a State, or in the archipelagic waters of an archipelagic State."²⁸⁷ Although the United States has not ratified UNCLOS, this is a definition that the United States has recognized as customary international law and binding on the United States.²⁸⁸ Plain and ordinary meaning should also be considered in evaluating the scope of the law by looking to the current meaning of plain text rather than notions of a term's meaning that have since been superseded. The current UNCLOS' meaning of "high seas" was not in existence in 1972 when the MMPA was enacted or in 1973 when the ESA was enacted.²⁸⁹ At the time of MMPA and ESA enactment, the term was understood to include the definition under the 1958 Convention on the High Seas of "all parts of the sea that are not included in the territorial sea or in the internal waters of a State."²⁹⁰ Arguably, this could encompass EEZs, but these areas were not established yet.²⁹¹ And it is clear that UNCLOS has since superseded the 1958 Convention on the High Seas.²⁹²

²⁸⁵ UNCLOS, *supra* note 6, art. 56(1)(b).

²⁸⁶ BLACK'S LAW DICTIONARY 1349 (7th ed., 1999).

²⁸⁷ UNCLOS, *supra* note 6, art. 86.

²⁸⁸ See *Mayaguezanos por la Salud y el Ambiente v. United States*, 38 F. Supp. 2d 138, 175 & n.3 (D.P.R. 1999), *aff'd* 198 F.3d 297, 305 & n.14 (1st Cir. 1999); *R.M.S. Titanic, Inc. v. Haver*, 171 F.3d 943, 965 n.3 (4th Cir. 1999).

²⁸⁹ This current definition is reflected in the 1982 UNCLOS.

²⁹⁰ 1958 Convention on the High Seas, Apr. 29, 1958, 13 U.S.T. 2312, T.I.A.S. NO. 5200, 559 U.N.T.S. 285.

²⁹¹ "Exclusive Economic Zone" first appeared during the negotiations of the Third United Nations Conference on the Law of the Sea Convention in 1975. See ESSAYS IN MEMORY OF JEAN CARROZ: THE LAW OF THE SEA (UN FAO ed. 1987), available at <http://www.fao.org/docrep/s5280T/s5280t0p.htm#the%20exclusive%20economic%20zone:%20a%20historical%20perspective> (last visited Oct. 25, 2009).

²⁹² See UNCLOS, *supra* note 6, preamble (indicating that the parties wanted to "[n]ot[e] that developments since the United Nations Conferences on the Law of the Sea held at Geneva in 1958 and 1960 have accentuated the need for a new and generally acceptable Convention on the law of the sea") (emphasis in original).

Furthermore, the presumption against extraterritoriality of the MMPA is not foreclosed just because the statute's language appears to address the issue. To the contrary, under *Smith v. United States*, the Supreme Court has stated that the presumption can even withstand express language appearing to address the extraterritorial application, and all statutory terms likely to expand the law's scope beyond U.S. territory should be construed narrowly to the extent reasonably possible.²⁹³ In total, the term "high seas" within the MMPA and the ESA should not be read to include EEZs.

VII. CONCLUSION

With the United States promoting a policy in the Arctic of regional partnerships with other sovereign nations through its involvement in the Arctic Council and all Arctic nations researching their outer limits of maritime claims within the Arctic, shifting boundaries may mean alterations in domestic law application. If climate change opens the waters of the Arctic, U.S. agency activity in the area will likely increase pre-activity planning and, therefore, application of the NEPA, MMPA and ESA. Applying these domestic laws to Arctic activities will require a delicate balance to ensure protection of the environment but not intrude on other nations' sovereignty or the efforts of the Arctic Council. The presumption against extraterritoriality still is applicable to bar the NEPA's application outside the territory and territorial sea of the United States, despite being a procedural statute. The presumption is not lost merely because there is no conflict of laws. The Supreme Court has noted that the presumption is rooted in another consideration—The fact that generally Congress legislates with domestic concerns in mind.²⁹⁴ U.S. agencies in charge of overseeing implementation of the MMPA and ESA tend to push application of these statutes extraterritorially beyond their current coverage limits. This unjustified application has the potential to frustrate the diplomatic efforts of the United States in fostering a regional cooperative scheme. These expert agencies and other non-governmental advocates may push such applications to the point where court interpretation or amendment of the federal laws forces conclusion of the issue. But United States ratification of UNCLOS may help agencies recognize that the domestic laws governing the maritime environment must comport with the framework for the maritime zones developed by the international community, including the United States. Although the NEPA, ESA, and MMPA were enacted prior to the UNCLOS in force today, the treaty's codification of customary law must control when interpreting the ordinary and

²⁹³ *Smith v. United States*, 507 U.S. 197, 203-04 (1993) (interpreting the phrase "foreign country" narrowly to restrict application of the Federal Tort Claims Act outside the United States).

²⁹⁴ *See id.*

normal meaning of undefined terms such as “high seas” within these statutes. The presumption against extraterritoriality remains applicable to the NEPA to require Executive Order 12114 application rather than the NEPA outside the territorial sea of the United States. And the presumption applies also to MMPA and ESA, to deny application in foreign EEZs and foreign territorial seas. The U.S. EEZ is clearly within the “water of the jurisdiction of the United States” under the MMPA, but it is less clear whether the ESA was meant by Congress to extend to the U.S. EEZ, a later-in-time designated area. The ordinary meaning of EEZ generally does not include it within the territorial sea. And the term “high seas” with these statutes has an ordinary meaning as generally accepted under UNCLOS to exclude areas considered EEZs since Congress did not fix the term in geographic scope. Nevertheless, in undertaking federal agency environmental planning in the Arctic, action agencies should be aware of potential over-broad application of the MMPA and ESA.

THE SHIPBOARD PANDORA'S BOX: THE OPERATIONAL REALITY THAT AN EXPECTATION OF PRIVACY EXISTS IN ELECTRONIC COMMUNICATIONS ABOARD NAVAL VESSELS

Lieutenant Colonel Leon James Francis¹

I. INTRODUCTION

Life on a United States Naval vessel when deployed is typically slow and monotonous.² For months at a time, the ship is the Sailor's or Marine's place of work, worship, dining, and entertainment.³ Life aboard ship is not only the job; it is also home. Personal privacy is limited.⁴ There is no place to get away from the ship when the ship is at sea. Life at sea has unique and significant constraints.⁵ While embarked, communications with anyone not on the ship must be done almost exclusively using the ship's communication

¹ Judge Advocate, United States Marine Corps. Presently assigned as Head, Military Law Branch, Judge Advocate Division, Headquarters Marine Corps. LL.M. 2009, The Judge Advocate General's School, Charlottesville, Va.; J.D. 1996, Gonzaga University School of Law; B.A., 1993, Boise State University. Previous assignments include: Staff Judge Advocate, 11th Marine Expeditionary Unit, I Marine Expeditionary Force, Camp Pendleton, California, 2006-2008; Legal Services Support Section, Camp Pendleton, California, 2003-2006 (Senior Defense Counsel, 2005-2006; Officer-in-Charge, Legal Team E, 2004; Senior Trial Counsel, Legal Team E 2003-2004); Officer-in-Charge, Legal Team Camp Hansen, Legal Services Support Section, 3d Force Service Support Group, Okinawa, Japan, 2002-2003; Deputy Staff Judge Advocate, 3d Marine Division, Okinawa, Japan, 2000-2002; Marine Corps Air Station, Yuma, Arizona, 1998-2000 (Chief Trial Counsel/Special Assistant United States Attorney 1999-2000; Trial Counsel/Administrative Law Officer 1998-1999). Member of the Idaho State Bar. This article was submitted in partial completion of the Master of Laws requirements of the 57th Judge Advocate Officer Graduate Course.

² See generally S.F. TOMAJCZYK, MODERN U.S. NAVY DESTROYERS 29 (2001) (describing the amenities and services offered during a sea-based deployment to counter long deployments).

³ See generally DOUGLAS C. WALLER, BIG RED: THREE MONTHS ON BOARD A TRIDENT NUCLEAR SUBMARINE 190 (2001) (explaining the everyday activities of a Sailor aboard a United States submarine, in comparison to life aboard a ship).

⁴ *Id.* at 7 ("As in a family, there were no secrets on the *Nebraska*. . . . No privacy. Enlisted men sized up officers within a day. Gossip spread quickly. Everyone lived in everyone else's dirty laundry, literally as well as figuratively. Everyone knew everyone else's business. Everyone watched everyone else.").

⁵ See JAMES STAVRIDIS, DESTROYER CAPTAIN: LESSONS OF A FIRST COMMAND 32-34 (2008) (depicting the average day and week aboard ship and how morale is a significant consideration for a commander).

systems, including the Internet, e-mail, telephones, and video-teleconferencing equipment.⁶

What makes this way of life unique is the significant reliance the individual servicemember must place on government resources to make contact with the outside world. During a deployment to a forward-operating base, commercial companies provide alternatives for service members to make personal communications other than with the use of government communication systems. For example, a forward-operating base will have privately operated Internet cafes or telephone centers for service members to make private, personal communications.⁷ When deployed aboard a naval vessel, sailors and marines have few such options.

In light of this dilemma, commanders and system administrators will generally grant greater leeway in the use of government systems for personal communication while embarked aboard ships.⁸ Sailors and Marines can, and are expected to, use their government e-mail accounts to maintain regular contact with their families, send messages to friends, and conduct personal business.⁹ Time is set aside daily in the ship's routine to open up the Internet for the use of non-governmental educational and financial websites.¹⁰ As a morale booster, Sailors and Marines are even permitted to use ship's telephones and video-teleconferencing systems to call home periodically.¹¹ These leeways, though, could have the effect of creating a legally protected expectation of privacy in personal communications made using these systems.

The practice of allowing, and in some cases requiring, Sailors and Marines to make personal communications using government communication systems while deployed at sea can create a constitutionally protected expectation of privacy. In the recent case of *United States v. Long*, the United States Court

⁶ E-mail from Lieutenant Colonel G. G. Malkasian, USMC, Commanding Officer, Second Recruit Training Battalion, Recruit Training Regiment, MCRD San Diego, to Major L. J. Francis, USMC (Oct. 28, 2008, 15:39 EST) (on file with author). LtCol Malkasian was the Communications Officer for the 11th Marine Expeditionary Unit during its sea-based deployments aboard the USS Pelilieu (LHA 5) in 2006 and USS Tarawa (LHA 1) from 2007 to 2008. *Id.*

⁷ 13TH MARINE EXPEDITIONARY UNIT, ORDER 5500.1, DEPLOYED DIGITAL MEDIA POLICY para. 6 (13 Oct. 2008) (discussing the availability of commercial communications when forward deployed upon debarkation of the ship).

⁸ Malkasian, *supra* note 6.

⁹ E-mail from Sergeant Major Shannon K. Johnson, USMC, Sergeant Major, 11th Marine Expeditionary Unit, to Major L. J. Francis, USMC (Jan. 14, 2009, 13:53 EST) (on file with author). SgtMaj Johnson has deployed at sea four times in his career to include three times as a sergeant major. *Id.* A Marine Expeditionary Unit is a part of an Amphibious Ready Group that deploys aboard three ships at a time. *Id.* As a result, SgtMaj Johnson has interacted with twelve different ships during his career during four sea-based deployments. *Id.*

¹⁰ Malkasian, *supra* note 6.

¹¹ *Id.*

of Appeals for the Armed Forces (“CAAF”) recognized that certain practices of government officials could create an expectation of privacy in electronic communications made using government systems.¹²

This article argues that, due to current practices and operational realities, a limited, protected expectation of privacy does exist in certain personal, shipboard, electronic communications. This right should be retained, though, because it contributes to the proper functioning of a unit deployed at sea in that it lifts morale and thereby enhances a commander’s ability to maintain good order and discipline. Part II reviews the constitutional law of privacy and its limited application in the military context. Part III depicts the difficulties of service members, and their commanders, in maintaining communication with family, avoiding boredom, and sustaining morale while embarked aboard a vessel. Part IV analyzes the new Department of Defense (“DOD”) privacy policy in light of *Long* and argues for the need to maintain a limited expectation of privacy at sea. Part V concludes that personal privacy expectations can coexist with operational security in an embarked environment and proposes remedies for misuse.

II. EXPECTATION OF PRIVACY IN THE MILITARY

The Fourth Amendment to the United States Constitution states, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause”¹³ While this right applies clearly to civilians, the Supreme Court has said that constitutional rights apply differently to service members in order to maintain good order and discipline:

In the armed forces some restrictions exist for reasons that have no counterpart in the civilian community. . . . The armed forces depend on a command structure that at times must commit men to combat, not only hazarding their lives but ultimately involving the security of the Nation itself.¹⁴

In *Parker v. Levy*, the Supreme Court addressed First Amendment freedom of speech and the ability to restrict it in the military community if it undermines the effectiveness of command.¹⁵ Comparing this to the Fourth Amendment, the right to be free from unreasonable searches and seizures can also, at times, apply differently in the military. In examining how the Fourth

¹² 64 M.J. 57, 64 (2006).

¹³ U.S. CONST. amend. IV.

¹⁴ *Parker v. Levy*, 417 U.S. 733, 758-59 (1974).

¹⁵ *Id.* at 759.

Amendment applies to the military, a discussion of its general applicability is required.

A. Expectation of Privacy Generally

The Fourth Amendment only protects against *unreasonable* searches and seizures, not all searches and seizures.¹⁶ Before a protection from government intrusion arises the individual must have a reasonable expectation of privacy in the place to be searched or thing to be seized.¹⁷ In determining whether an expectation of privacy is reasonable, two questions are raised. The first question is subjective: Did the individual *honestly* have an expectation of privacy in the place searched or items seized?¹⁸ The second question is objective: Is the expectation of privacy that the individual honestly held one that *society* is willing to accept as *reasonable*?¹⁹ If both questions are answered in the affirmative, then Fourth Amendment protections apply and judicial relief, in the form of excluding illegally-seized evidence, may be available.²⁰

Places typically held to satisfy the second question of the reasonableness test are houses,²¹ curtilage,²² and tenements,²³ to name a few. The Supreme Court has also recognized that a protected expectation of privacy exists in certain types of private communications using electronic devices, such as private telephone conversations.²⁴ In *Katz*, the Court addressed whether there existed a protected expectation of privacy from government intrusion in a telephone conversation using a public telephone booth.²⁵ The petitioner was convicted of transmitting wagering information by telephone from Los Angeles to Miami and Boston, a federal crime.²⁶ FBI agents collected significant pieces of incriminating evidence, including the petitioner's conversations in a public

¹⁶ For a discussion of recent developments in search and seizure law pertaining to the military, see generally Lieutenant Colonel S. R. Stewart, USMC, *Katy Bar the Door—2006 New Developments in Fourth Amendment Search and Seizure Law*, ARMY LAW., June 2007, at 10-11.

¹⁷ For a thorough background of the Fourth Amendment, see Lieutenant Commander R. A. Conrad, *Searching for Privacy in All the Wrong Places: Using Government Computers to Surf Online*, 48 NAVAL L. REV. 1, 6-8 (2001).

¹⁸ See *Katz v. United States*, 389 U.S. 347, 352 (1967) (emphasis added).

¹⁹ See *id.* (emphasis added).

²⁰ *Id.* Illegally seized means in the absence of a warrant, search authorization or legally recognized exception. See *id.*

²¹ *Silverman v. United States*, 365 U.S. 505 (1961).

²² See WAYNE R. LAFAYE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 465 (3d ed. 1996).

²³ See *Arizona v. Hicks*, 480 U.S. 321 (1987) (discussing the expectation of privacy in stereo equipment seized in an apartment).

²⁴ *Katz v. United States*, 389 U.S. 347, 352 (1967).

²⁵ *Id.* at 348.

²⁶ *Id.*

telephone booth, to the outside of which the agents attached a listening device.²⁷ The Court shed light on a standing judicial misconception between “constitutionally protected areas” and the Fourth Amendment’s actual protection from unreasonable searches.²⁸ Delivering the opinion of the Court, Justice Stewart sought to dispel this misconception:

The petitioner has strenuously argued that the booth was a “constitutionally protected area.” The Government has maintained with equal vigor that it was not. But this effort to decide whether or not a given “area,” viewed in the abstract, is “constitutionally protected” deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.²⁹

The Court concluded that telephone conversations between individuals intended by the participants to be private are included within the protective sweep of the Fourth Amendment.

The Supreme Court has not yet addressed the issue of Internet communications. Other civilian courts have addressed it, though. The United States Court of Appeals for the Ninth Circuit has analogized e-mail and text messaging to letters in the Fourth Amendment context.³⁰ In *Quon v. Arch Wireless Operating Co., Inc.*, Sergeant Quon of the Ontario, California Police Department sued Arch Wireless, a text messaging provider, under the Stored Communications Act³¹ and the Fourth Amendment over the release of certain personal text messages, of a questionable nature, to officials of the Ontario government.³² The text message provider was contracted through the city and the subject text messages were sent using devices and services procured under that contract.³³ The City of Ontario had a “Computer Usage, Internet and E-Mail Policy” which employees, including Sergeant Quon, had to acknowledge in writing.³⁴ The policy stated no expectation of privacy or confidentiality existed in city Internet or e-mail systems, including text messaging, and e-mail and

²⁷ *Id.*

²⁸ *Id.* at 351.

²⁹ *Katz*, 389 U.S. at 351 (internal citations omitted).

³⁰ *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 905 (9th Cir. 2008).

³¹ 18 U.S.C. §§ 2701-2711 (2006).

³² *Quon*, 529 F.3d at 895-96.

³³ *Id.*

³⁴ *Id.* at 896.

Internet use could be monitored at any time without notice.³⁵ Counter to the written policy, the police department's practice was that it would not monitor its department's pagers or any text messages so long as any personal use was reimbursed to the city.³⁶

As the Ninth Circuit found, an individual can have a reasonable expectation of privacy in the contents of a sealed letter, but not in the markings on the outside of that letter which can be seen by anyone who may pick it up.³⁷ Likewise, the address on a sent e-mail or text message is not protected because, just like an address placed on the outside of a letter, the intent is for it to be used by others to deliver the message to the correct addressee.³⁸ The internal contents of the e-mail or text message are protected by the Fourth Amendment, though, so long as the individual has an honestly held expectation of privacy in those contents.³⁹ However, when compared to the unique military context, these rules could have a different application when applied to service members.

B. The Military Exception and its Limits

The U.S. Court of Appeals for the District of Columbia Circuit applied the *Parker v. Levy*⁴⁰ civilian-military constitutional dichotomy to the Fourth Amendment in *Committee for GI Rights et al., v. Callaway*.⁴¹

GIs are entitled to the protection of the Fourth Amendment as are all other American citizens. . . . [H]owever, the specific content and incidents of [one's rights under the Fourth Amendment] must be shaped by the context in which [they are] asserted. Reasonableness is the controlling standard. What is reasonable in one context may not be reasonable in another. . . . To strike the proper balance between legitimate military needs and individual liberties we must inquire

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Quon*, 529 F.3d at 905 (citations omitted).

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ 417 U.S. 733, 759 (1974). Captain Levy was a physician who was convicted of violations of Articles 133 and 134, Uniform Code of Military Justice (UCMJ), for discouraging African-American Soldiers from following orders to participate in the Vietnam Conflict. *Id.* The main issue in the case was whether Articles 133 and 134, UCMJ, were overbroad and unconstitutional in violation of the First Amendment. *Id.* The Supreme Court ruled they were not overbroad and that the First Amendment applied differently to those in the military than those in general society because speech that is otherwise protected in civilian society "may nonetheless undermine the effectiveness of [military] command." *Id.*

⁴¹ 518 F.2d 466 (D.C. Cir. 1975).

whether conditions peculiar to military life dictate affording different treatment to activity arising in a military context.⁴²

Based upon this reasoning, the D.C. Circuit concluded that a soldier's expectation of privacy is diminished in certain circumstances.⁴³ In *Callaway*, eighteen soldiers in the United States Army's European Command filed a class action contending that certain illegal drug prevention and barracks control programs were unconstitutional.⁴⁴ Regarding barracks controls, the soldiers challenged the command policy that allowed subordinate commanders to prohibit "the display on barracks walls of posters which in their judgment constitute a danger to military loyalty, discipline and morale."⁴⁵ The D.C. Circuit disagreed: "The soldier cannot reasonably expect the Army barracks to be a sanctuary like his civilian home."⁴⁶

Applying a similar analysis, military courts have determined that soldiers, sailors, airmen and marines have a diminished expectation of privacy in certain venues. In *United States v. Battles*, the Court of Military Appeals ("CMA") determined that a sailor has no reasonable expectation of privacy in common areas of a berthing space that are shared and heavily trafficked.⁴⁷ In *Battles*, a sailor asserted that he was subject to an improper health and comfort inspection.⁴⁸ The sailor, along with others on his ship, USS Enterprise (CVN 65), had been suspected of illegal drug involvement by his command.⁴⁹ When a box containing LSD was found aboard the ship, the ship's executive officer ordered a "health and comfort" inspection of berthing.⁵⁰ During the inspection, a box belonging to Storekeeper Seaman Apprentice Battles was found on the floor, near a maintenance locker in the berthing area.⁵¹ This berthing area was shared with sixty other Sailors in an area that was heavily trafficked to reach other areas of the ship.⁵² When they seized the box, officials discovered Phenobarbital, a controlled substance, and various lighters belonging to the ship inside.⁵³

SKSA Battles argued that the "health and comfort" inspection was a subterfuge and that he had a Fourth Amendment expectation of privacy in his

⁴² *Id.* at 476 (internal citations omitted).

⁴³ *Id.* at 477.

⁴⁴ *Id.* at 467.

⁴⁵ *Id.* at 470.

⁴⁶ *Cmte. for G.I. Rights*, 518 F.2d at 477.

⁴⁷ 25 M.J. 58, 60 (C.M.A. 1987).

⁴⁸ *Id.* at 59.

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² *Battles*, 25 M.J. at 59.

⁵³ *Id.*

berthing space.⁵⁴ The CMA disagreed: “A berthing area on a naval ship is more like a workplace than a home or barrack’s [sic] environment. We hold that operational realities and common sense dictate that, at the very least, appellant had no reasonable expectation of privacy in the common spaces of such a berthing area.”⁵⁵

The CMA further explored the *Callaway* rule in *United States v. McCarthy*.⁵⁶ In *McCarthy*, the Court of Military Appeals stated, “[w]hile the physical trappings of a modern barracks or military dormitory may be more comfortable and private than an open bay barracks, the need for discipline and readiness has not changed.”⁵⁷ There, the issue was whether an airman could retreat to his barracks room to avoid a warrantless apprehension; the Court of Military Appeals ruled he could not.⁵⁸ A military policeman patrolled the appellant’s barracks after recent reports that an approximately six-foot-tall, dark-skinned man with a tattoo and wearing a ski mask had assaulted three female airmen residing in a nearby military dormitory.⁵⁹ After receiving physical descriptions from witnesses that matched the physical characteristics of Airman McCarthy, the MP went to Airman McCarthy’s barracks room.⁶⁰ After knocking on the door without an answer, he entered the room and attempted to wake Airman McCarthy, whom he saw lying on a bunk.⁶¹ He then turned over Airman McCarthy and found a ski mask tucked in his waistband.⁶² The court hung the expectation of privacy in a barracks room upon the second question of the *Katz* analysis, that is, whether society deems the privacy sought as reasonable.⁶³ As a result, an expectation of privacy in the military can vary greatly depending upon the circumstances.

Regarding sealed letters, however, service members enjoy the same expectation of privacy as civilians.⁶⁴ In *United States v. Springer*, CAAF announced that “[a]s a general rule, persons joining the armed forces do not forfeit the same reasonable expectation of privacy in the contents of their mail enjoyed by other members of American society they serve and protect.”⁶⁵ In *Springer*, Air Force Staff Sergeant Springer left a letter at the front desk in a

⁵⁴ *Id.*

⁵⁵ *Id.* at 60.

⁵⁶ 38 M.J. 398, 403 (C.M.A. 1993)

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ *Id.* at 399.

⁶⁰ *Id.*

⁶¹ *McCarthy*, 38 M.J. at 399.

⁶² *Id.*

⁶³ *Id.* at 401-03.

⁶⁴ *United States v. Springer*, 58 M.J. 164, 169 (C.A.A.F. 2003).

⁶⁵ *Id.*

trainee dormitory intending it to be mailed.⁶⁶ As a Combat Skills Instructor for a Security Officer's Apprentice Course, SSgt Springer was specifically prohibited from having personal relationships with students in the course.⁶⁷ Another staff sergeant, who was manning the desk, picked up the letter and looked at it to ensure the proper postage was affixed.⁶⁸ In doing so, he noticed that SSgt Springer was the sender and was sending it to a former student.⁶⁹ Upon closer inspection, he could see the inner contents of the letter plainly through the envelope, indicating that an unauthorized personal relationship existed between SSgt Springer and the former student.⁷⁰

The CAAF held there was no reasonable expectation of privacy in the letter because the contents of the letter were plainly visible to anyone who may pick it up and were not adequately concealed.⁷¹ In dicta, the court mused that, had SSgt Springer mailed the letter himself or used a thicker, more opaque envelope, a reasonable expectation of privacy in its contents would have existed.⁷²

“[An] e-mail is like a letter” in the way military courts analyze whether there is a protected expectation of privacy in its contents.⁷³ In *United States v. Maxwell*, CAAF held that a servicemember has a reasonable expectation of privacy under the Fourth Amendment in e-mails sent through private, personal e-mail accounts.⁷⁴ In *Maxwell*, an Air Force Colonel challenged the seizure of communications he made using his private America On-Line Account.⁷⁵ Here, the court distinguished between chat room communications and e-mail. Chat room conversations, or e-mails sent to the public at large, “lose any semblance of privacy,” but the contents of private e-mails are like letters in that their contents are protected from unreasonable government search and seizure.⁷⁶

In a broad sense, the Military Rules of Evidence (“MRE”) have tried to apply these general Fourth Amendment standards to the military environment. MRE 311(a)(2) states, “Evidence obtained as a result of an unlawful search or seizure made by a person acting in a governmental capacity is inadmissible

⁶⁶ *Id.* at 166-67.

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ *Springer*, 58 M.J. at 166-7.

⁷⁰ *Id.*

⁷¹ *Id.* at 169.

⁷² *Id.*

⁷³ *United States v. Maxwell*, 45 M.J. 406, 418 (1996).

⁷⁴ *Id.* at 419.

⁷⁵ *Id.* at 410-17.

⁷⁶ *Id.*

against the accused if . . . the accused had a reasonable expectation of privacy in the person, place or property searched . . .”⁷⁷ MRE 314(d) goes further:

Government property may be searched under this rule unless the person to whom the property is issued or assigned has a reasonable expectation of privacy therein at the time of the search. . . . [T]he determination as to whether a person has a reasonable expectation of privacy in government property issued for personal use depends on the facts and circumstances at the time of the search.⁷⁸

MRE 316(d)(3) allows government property to be seized “without probable cause and without a search warrant or search authorization . . . unless the person to whom the property is issued or assigned has a reasonable expectation of privacy therein.”⁷⁹ In sum, the MREs contemplate that under the right circumstances a servicemember can have a reasonable expectation of privacy in some uses of government property.

In this regard, some types of electronic communications using government communication systems are protected by the Fourth Amendment.⁸⁰ In *United States v. Long*, the CAAF determined that in certain circumstances a servicemember has a reasonable expectation of privacy in e-mails transmitted and stored using a government e-mail account.⁸¹ The determining factor that the court used in finding a reasonable expectation of privacy was the internal government agency’s practices and policies.⁸² In *Long*, a Lance Corporal used her government e-mail account to correspond with friends.⁸³ This type of personal use of her government-provided e-mail account was permitted, so long as it was not excessive and did not interfere with her duties.⁸⁴ In e-mails to friends, LCpl Long indicated her fear that her illegal drug use would be detected via urinalysis, and she described the steps she was taking to avoid such detection.⁸⁵ After she was suspected of misconduct, an investigator requested that the system administrator retrieve her e-mails.⁸⁶ At court-martial, an agency administrator testified that “[Headquarters, Marine Corps] policy regarding

⁷⁷ MANUAL FOR COURTS-MARTIAL, UNITED STATES, MIL. R. EVID. 311(a)(2) (2008) [hereinafter MCM].

⁷⁸ *Id.*, MIL. R. EVID. 314(d).

⁷⁹ *Id.*, MIL. R. EVID. 316(d)(3).

⁸⁰ *United States v. Long*, 64 M.J. 57 (2006).

⁸¹ *Id.* at 65.

⁸² *Id.* at 64.

⁸³ *Id.* at 59.

⁸⁴ *Id.* at 63.

⁸⁵ *Long*, 64 M.J. at 59.

⁸⁶ *Id.*

using the network to send personal e-mails had always been lenient and that such use of the network was considered authorized.”⁸⁷ When testing the network, though, he did not monitor individual accounts because “‘it’s a privacy issue.’”⁸⁸

When LCpl Long sent her incriminating e-mails, a Department of Defense (“DOD”) logon banner was in use.⁸⁹ The banner read that “All information, including personal information, placed or sent over this system may be monitored.”⁹⁰ Despite this warning, the CAAF held that LCpl Long did enjoy a protected expectation of privacy in her e-mails: “[T]he testimony of the network administrator is the most compelling evidence supporting the notion that Appellee had a subjective expectation of privacy. . . . [He] repeatedly emphasized the agency practice of recognizing the privacy interests of users in their e-mail.”⁹¹ As a result, if government officials allow personal communications on government-provided systems, it creates a reasonable subjective inference that those communications will be considered private, and a Fourth Amendment-protected expectation of privacy will arise.

Allowing limited personal use of a government computer, though, does not create a reasonable expectation of privacy in the computer itself.⁹² In *United States v. Larson*, CAAF limited its holding in *Long* by distinguishing between e-mail communications and the general use of a computer itself.⁹³ In *Larson*, an Air Force Major used his government computer to make instant message communications with a person he thought was an underage female, but actually was a civilian police detective working undercover to catch on-line predators of children.⁹⁴ Major Larson was later arrested and his government computer was searched.⁹⁵ Various images of child pornography were found stored on the computer’s hard drive along with other explicit evidence.⁹⁶

The CAAF found that Major Larson had no reasonable expectation of privacy in the computer because it was government-owned and government officials could access it at any time.⁹⁷ Unlike in *Long*, Major Larson presented no evidence that he “enjoyed an expectation of privacy in materials on his

⁸⁷ *Id.* at 65.

⁸⁸ *Id.*

⁸⁹ *Id.* at 60.

⁹⁰ *Long*, 64 M.J. at 60 (emphasis added).

⁹¹ *Id.* at 63.

⁹² *United States v. Larson*, 66 M.J. 212, 215 (2008).

⁹³ *Id.*

⁹⁴ *Id.* at 214.

⁹⁵ *Id.*

⁹⁶ *Id.*

⁹⁷ *Larson*, 66 M.J. at 215.

government computer,” and the testimony of his commander established both monitoring of and command access to the computer. In other words, it was not suggested to Major Larson that he could use the computer exclusively for his own private use.⁹⁸ Thus, Major Larson did not enjoy a protected Fourth Amendment expectation of privacy because he did not have a reasonable subjective belief that his use was private.⁹⁹

The most significant distinction between *Long* and *Larson* is the inference left in the mind of the government system user. In *Long*, the inference was that e-mails were personal and would not be randomly viewed or inspected, but in *Larson* there was no such legitimate inference. In *Long*, CAAF recognized that in certain circumstances a reasonable expectation of privacy can arise in electronic communications using government systems. This is an exception to the general rule that there is no expectation of privacy in government property or services. To counter this exception, though, the DOD has made recent attempts to mitigate the CAAF’s ruling by issuing a new policy statement regarding the personal use of government information systems.

C. The DOD’s Response to *Long*

In an attempt to eliminate the type of situation that gave rise to a protected expectation of privacy in government e-mail, as in *Long*, the DOD changed its policy and logon banner.¹⁰⁰ Prior to *Long*, the standard DOD logon banner stated:

DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. . . . All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other

⁹⁸ *Id.* at 215-16.

⁹⁹ *Id.* at 216.

¹⁰⁰ See Memorandum from Chief Information Officer, Department of Defense, to Secretaries of Military Departments et al., subject: Policy on Use of Department of Defense Information Systems-Standard Consent Banner and User Agreement (2 Nov. 2007) [hereinafter Memo from CIO]. This memorandum was later superseded in a memorandum dated 9 May 2008.

adverse action. Use of this system constitutes consent to monitoring for these purposes.¹⁰¹

In response to *Long*, the logon banner was revised as follows:

By using this [information system], you consent to the following conditions: The [U.S. Government] routinely monitors communications occurring on this [information system], and any device attached to this [information system], for purposes including, but not limited to, penetration testing, COMSEC monitoring, network defense, quality control, and employee misconduct, law enforcement, and counterintelligence investigations. At any time, the [U.S. Government] may inspect and/or seize data stored on this [information system] and any device attached to this [information system]. Communications occurring on or data stored on this [information system], or any device attached to this [information system] are not private. They are subject to routine monitoring and search. Any communications occurring on or data stored on this [information system], or any device attached to this [information system], may be disclosed or used for any [U.S. Government] authorized purpose. Security protections may be utilized on this [information system] to protect certain interests that are important to the [U.S. Government]. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the [U.S. Government]. These protections are not provided for your benefit or privacy and may be modified or eliminated at the [U.S. Government's] discretion.¹⁰²

The purpose of the change in the banner was to “make it clear that there is no expectation of privacy when using DoD information systems. . . even if some personal use of a system is permitted.”¹⁰³ The change seems to be at least partially influenced by Judge Crawford’s warning in her dissent in *Long*.¹⁰⁴ Though Judge Crawford made this recommendation, she still believed the logon banner as it existed was adequate to eliminate any objective expectation of

¹⁰¹ United States v. Long, 64 M.J. 57, 60 (2006).

¹⁰² Memo from CIO, *supra* note 100.

¹⁰³ *Id.*

¹⁰⁴ 64 M.J. at 68 (Crawford, J., dissenting) (“[A] rewording of subsequent DoD Internet usage banners may be advisable.”).

privacy.¹⁰⁵ The new DOD Policy, however, still protects certain private communications on government information systems, such as privileged communications.¹⁰⁶

This change to the DOD logon banner still fails to address the most significant reason why CAAF found that a protected expectation of privacy could exist in government e-mail. Regardless of policy, the conduct of government administrators can still create a protected expectation of privacy. As *Long* makes clear, it is this administrator conduct that controls whether a reasonable expectation of privacy arises in the use of a government electronic communication system. If such conduct creates a reasonable subjective expectation of privacy, then Fourth Amendment protections will still attach regardless of what a logon banner may state. This is exactly the problem when dealing with shipboard electronic communications. Due to the unique nature of life at sea, commanders and systems administrators are almost forced to allow limited, personal, private uses of shipboard communication systems in order to enhance morale and maintain good order and discipline.

III. LIFE AT SEA

Life at sea on board a United States Navy ship is typically depicted in books, movies and Navy recruiting commercials as romantic and adventurous, but the reality of life at sea is far from what is typically popularized.¹⁰⁷ The United States Navy has no equals. While in international waters, a United States Naval vessel has few threats of concern.¹⁰⁸ The lack of realistic operational threats while on the high seas makes daily life at sea slow and unexciting.

A. Day to Day

While deployed aboard a United States Naval vessel the often-used phrase “24/7” becomes a reality.¹⁰⁹ The ship is not only the Sailor’s or Marine’s place of work but also his or her home. There is little distinction between work and home while deployed. The Sailor or Marine may be called upon to fulfill

¹⁰⁵ *Id.* at 68-70 (Crawford, J., dissenting).

¹⁰⁶ See Memo from CIO, *supra* note 100 (“This policy is not intended to negate any privilege recognized by law. . .”).

¹⁰⁷ See generally STAVRIDIS, *supra* note 5, at 116 (describing a period of seventy-one days at sea as “brutal,” and a “sentence in jail” during a period of time when the author was the Commanding Officer of the USS Barry (DDG 52)).

¹⁰⁸ See generally TOMAJCZYK, *supra* note 2, at 17 (citing the *Naval Vessel Registry* describing how the collapse of the Soviet Union dissolved the most significant threat to the United States Navy and thus resulted in downsizing and the increase in missions involving police actions and humanitarian aid).

¹⁰⁹ See STAVRIDIS, *supra* note 5, at 32-34 (describing the long hours and little down time a sailor received while deployed aboard the USS Barry (DDG 52)).

duties at all hours of the day or night such as standing watch.¹¹⁰ When the Sailor or Marine gets personal time, there is really no place to spend it in a truly personal capacity.¹¹¹ Enlisted personnel are typically berthed in small cramped spaces on the lower decks of the ship.¹¹² The junior enlisted, typically in the rank of E-4 and below, are given bunks which are stacked three high.¹¹³ A typical berthing space is “twenty-seven-inch[es]-wide, eighty-inch[es]-long, and twenty-ones-inch[es] high. . . .”¹¹⁴ Each bunk is not even as wide as a typical twin bed.¹¹⁵ The space from one row of bunks to those directly across from them can be less than three feet.¹¹⁶ In a typical berthing section there might be more than twelve Sailors or Marines occupying approximately 170 square feet of living space.¹¹⁷ Such conditions allow very little opportunity for any type of privacy. In addition, due to the risk of fire aboard ship in these cramped conditions, the ability of Sailors or Marines to use personal electronics is limited.¹¹⁸

Senior enlisted have slightly better living conditions. While still being placed in areas with bunks stacked three high, there are typically fewer persons berthed in these areas that allow for more square footage of living space per person.¹¹⁹ Instead of twelve Sailors or Marines, as in the junior enlisted berthing, senior enlisted may only share their 170 square feet of living space with six others.¹²⁰ As with junior enlisted, though, their opportunity for personal privacy is limited.

Officers have it better. Officers get staterooms, which are small and, unless the officer is a part of the command group (Commanding Officers and Executive Officers), usually shared with up to four other persons.¹²¹ Again, the living space is limited and the rooms get crowded. In such conditions, while

¹¹⁰ *Id.*

¹¹¹ See WALLER, *supra* note 3, at 7 (describing the lack of privacy while deployed at sea).

¹¹² See TOMAJCZYK, *supra* note 2, at 14 (showing a photograph of a berthing space aboard a United States destroyer); see also WALLER, *supra* note 3, at 8 (describing cramped berthing accommodations).

¹¹³ Johnson, *supra* note 9.

¹¹⁴ WALLER, *supra* note 3, at 8.

¹¹⁵ *Id.*

¹¹⁶ See TOMAJCZYK, *supra* note 2, at 14 (showing a photograph of a berthing section aboard a United States destroyer).

¹¹⁷ Compare WALLER, *supra* note 3, at 8 (giving the dimensions of a typical berthing space) with TOMAJCZYK, *supra* note 2, at 14 (depicting the typical berthing area aboard a destroyer which indicates that up to twelve persons could occupy the same shared berthing area.)

¹¹⁸ Patrick Long, *Diary of a Sea-Going Sailor, Part 7, Ships Safety*, <http://usmilitary.about.com/cs/navy/a/diarysailor7.htm> (last visited Feb. 15, 2010).

¹¹⁹ Johnson, *supra* note 9.

¹²⁰ *Id.*

¹²¹ *Id.*

better than junior and senior enlisted berthing, any significant level of personal privacy is nonexistent.

Aside from the berthing areas, Sailors and Marines, when not working in their duty sections, can go to their respective lounges, the mess decks, or the gym. The enlisted lounge aboard a Naval vessel is usually small and crowded.¹²² It typically has a television that provides network news, sports channels, and Armed Forces Network programming.¹²³ In international waters when television signals cannot be received, the ship can only broadcast movies.¹²⁴ These movies are provided by the ship's Morale, Welfare and Recreation Representative. During a six-month deployment, the ship may repeatedly play the same movie on ship's television. The officer lounge is not much better. While usually less crowded due to a ship typically embarking fewer officers, it can still be hard to find a space to relax.

The eating areas (mess decks for junior enlisted, chiefs' mess for senior enlisted ranked E-7 and above, and wardroom for officers) are typically open only during meal hours.¹²⁵ At other times of the day they are used for holding meetings or teaching classes.¹²⁶ They are typically not a place for socializing.¹²⁷ The rules in the wardroom are a little more relaxed, but on the mess decks, enlisted are highly discouraged from being in the area unless on official matters or during meal hours.¹²⁸ The mess decks are also usually small and crowded. On the USS Tarawa (LHA 1) it was not uncommon for lines of Sailors and Marines to stretch from the mess decks (center of ship) to the forward part of the ship, in excess of fifty feet, waiting for a seat to empty so they could eat a meal.¹²⁹

The gymnasium is also crowded.¹³⁰ A smaller ship means a smaller gymnasium.¹³¹ Even though the equipment is typically modern (treadmills, stair steppers, stationary bicycles, universal machines, and many sets of free weights with benches), their numbers are limited compared to the number of Sailors or Marines deployed.¹³² On the USS Tarawa (LHA 1) and USS Pelilieu (LHA 5),

¹²² See generally TOMAJCZYK, *supra* note 2, at 29 (depicting sailors at rest).

¹²³ See generally *id.* (describing the availability of television aboard ship).

¹²⁴ *Id.*

¹²⁵ See generally WALLER, *supra* note 3, at 153-62 (describing the traditions of the wardroom aboard a naval vessel).

¹²⁶ *Id.*

¹²⁷ See generally Johnson, *supra* note 9 (discussing space on the mess deck).

¹²⁸ *Id.*

¹²⁹ *Id.*

¹³⁰ See generally TOMAJCZYK, *supra* note 2, at 29 (depicting crowded areas of the ship).

¹³¹ See generally WALLER, *supra* note 3, at 57 (describing the placement of exercise equipment).

¹³² Johnson, *supra* note 9.

up to 2000 Sailors and Marines could be deployed aboard at a given time.¹³³ The gymnasium could comfortably hold about fifty at a given time. This requires some ships that embark both Sailors and Marines to go to what is called blue/green hours. This means there are designated times when only Sailors can occupy the gym and other designated hours when only Marines can occupy the gym. Some ships break this down even further, by rank. Finding personal space on the ship, though, is not the only challenge for service members deployed at sea. Communicating with anyone not on the ship is also difficult.

All communications off of the ship must be made using ship-provided communication systems.¹³⁴ This is a stark contrast from land-based deployments. Even those deployed to forward-operating bases in Kuwait, Iraq, and Afghanistan have an opportunity to use non-governmental systems to communicate via the telephone or Internet.¹³⁵ Forward operating bases typically have telephone centers operated by commercial carriers, like AT&T, or commercially operated Internet cafes to allow service members to make personal contact with whomever they desire.¹³⁶ Service members at these forward operating bases can use their own personal computers in these Internet cafes to send e-mails or surf the Internet.¹³⁷ Sailors and Marines deployed aboard ship do not have these opportunities.

While at sea, the only computer system that is allowed to operate is the ship's computer system.¹³⁸ A Sailor or Marine is not allowed to plug a personal computer into this system.¹³⁹ Even the telephone lines are all government-provided.¹⁴⁰ There are commercial telephones available, but the signals leave the ship using the ship's satellite transmitters, not a commercial transmitter placed upon the ship.¹⁴¹ For example, there will be telephone booths or certain telephones designated for commercial purposes. In order to use these telephones the user must purchase a special telephone card, typically only sold aboard ship, in order to access the line.¹⁴² The cost of making a call is about fifty cents a minute, but the transmission is sent using a government transmitter to the commercial satellite.¹⁴³ If the transmitter is out of range, then the telephones

¹³³ *Id.*

¹³⁴ Malkasian, *supra* note 6.

¹³⁵ 13TH MARINE EXPEDITIONARY UNIT, ORDER 5500.1, DEPLOYED DIGITAL MEDIA POLICY para. 6 (13 Oct. 2008).

¹³⁶ Malkasian, *supra* note 6.

¹³⁷ See 13TH MEU ORDER, *supra* note 135, at para. 6 (describing the use of personal computers upon debarkation while deployed ashore).

¹³⁸ Malkasian, *supra* note 6.

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² *Id.*

¹⁴³ Malkasian, *supra* note 6.

will not work, which occurs in international waters frequently.¹⁴⁴ The high cost is generally prohibitive for the most junior Sailors and Marines to make regular contact with family back home.¹⁴⁵

All of these restrictions on personal privacy aboard ship have the potential to seriously undermine morale, thus creating increased difficulty in maintaining good order and discipline. In order to maintain morale, commanders offer many types of programs to keep Sailors and Marines engaged. Many of these programs require the use of ship communication systems to succeed.

B. Maintaining Morale

In order to maintain morale during a deployment aboard a United States Naval vessel, commanders offer many programs using the ship's communication systems. One of the most significant programs is the AFLOAT Educational Program.¹⁴⁶ This program gives Sailors and Marines the opportunity to take college courses while deployed at sea.¹⁴⁷ The program is accredited through Central Texas College.¹⁴⁸ The instructors are either other deployed service members who have a Bachelors or Masters level degree or actual civilian faculty who are embarked aboard ship.¹⁴⁹ Classes are typically held aboard ship in the evenings.¹⁵⁰ Since personal computers cannot be plugged into the ship's computer system, students must rely on government computers, systems and software in order to complete research projects or write papers for their courses.¹⁵¹

¹⁴⁴ *Id.*

¹⁴⁵ Johnson, *supra* note 9.

¹⁴⁶ 11TH MARINE EXPEDITIONARY UNIT, EDUCATION OFFICER TURNOVER BINDER (2007). On the West Coast, a Marine Expeditionary Unit Staff Judge Advocate is required to be the Education Officer for the unit. This is a collateral duty and requires the Education Officer to advertise the AFLOAT program to the unit prior to deployment. This includes searching for prospective instructors among the subordinate elements, compiling lists of available courses and providing registration information to prospective students. *Id.*

¹⁴⁷ *Id.*

¹⁴⁸ *Id.*

¹⁴⁹ *Id.* There are many classes offered, including College Algebra; Principles of Business Administration; United States History; Criminal Procedure and Psychology. 11TH MARINE EXPEDITIONARY UNIT, EDUCATION OFFICER TURNOVER BINDER (2007).

¹⁵⁰ *Id.*

¹⁵¹ See E-mail from Lieutenant Commander Kari A. Premus, USN, Communications Officer, Naval Surface Forces, to Major L. J. Francis, USMC (Jan. 12, 2008, 12:35 EST). LCDR Premus has served as the Communications Officer for the USS Pelilieu (LHA 5) and the USS Constellation (CV 64), and Electronic Maintenance Officer for the USS Arthur W. Radford (DD 968) and USS Mount Whitney (LCC 20). *Id.*

In addition, to allow the average Sailor or Marine to maintain access to the outside world, commanders will designate times when the Internet will be available for personal use because there is limited bandwidth aboard ship.¹⁵² The more users that are permitted on the Internet, the slower the Internet will run. As a result, communication officers are directed to limit users and available sites based upon the time of day.¹⁵³ For example, at certain times of day, access to the Internet will be limited to educational or banking sites only.¹⁵⁴ This gives Sailors and Marines an opportunity to get school work and personal banking done without the worry of slow service due to overworked servers.¹⁵⁵

The Internet can also be used to send personal e-mails.¹⁵⁶ Sailors and Marines are not allowed to access commercially available e-mail providers like Hotmail or Yahoo! while aboard ship.¹⁵⁷ The reason for this is to maintain operational security and to avoid computer viruses.¹⁵⁸ As a result, the only Internet e-mail available to send messages to family and friends is the ship's unclassified service.¹⁵⁹ This service is typically provided for only official government business, but while deployed the use of e-mail is expanded to allow for personal communications to maintain morale among both the deployed servicemember and his or her family.¹⁶⁰ It is neither unusual nor unexpected that a Sailor or Marine would exchange multiple e-mails with family members or friends in a single day.¹⁶¹ This is the norm. It keeps Sailors and Marines satisfied that they know what is going on at home, while keeping their families and loved ones satisfied that they know what is happening with their deployed Sailor or Marine. This continuous contact lessens the impact of the deployment on Family Readiness Personnel who remain behind and on the command in dealing with family concerns because the service members can deal with most

¹⁵² *Id.*; see also PRESTON GRALLA, HOW THE INTERNET WORKS 327 (7th ed. 2004) (defining bandwidth as "[a] measure of the amount of data that can be sent across an Internet connection over a unit of time").

¹⁵³ *Id.*

¹⁵⁴ *Id.*

¹⁵⁵ *Id.*

¹⁵⁶ See STAVRIDIS, *supra* note 5, at 80 (describing how he allowed morale and welfare telephone calls and personal communication with family via the Internet aboard his ship even back in mid-1990s while he was the Commanding Officer of the USS Barry).

¹⁵⁷ Johnson, *supra* note 9.

¹⁵⁸ *Id.*

¹⁵⁹ Malkasian, *supra* note 6. This service is commonly known as the "non-classified internet protocol router network," or NIPR. *Id.*

¹⁶⁰ See Conrad, *supra* note 17, at 24 (describing and citing specific guidelines (Message, 042354Z May 00, Commander in Chief, Atlantic Fleet, subject: Internet Policy) in the U.S. Navy "promot[ing] the widest permissible use of government information systems to access . . . the Internet, browse the World Wide Web, and communicate via electronic mail").

¹⁶¹ Johnson, *supra* note 9.

issues themselves.¹⁶² As Robert J. Carey, the Department of the Navy Deputy Chief Information Officer for Policy and Integration said,

Personal use of Navy equipment is good for morale, and it's reasonable to allow people to use Navy computers for non-work related purposes, as long as abuses are curbed. . . . Acceptable use of Navy IT equipment includes allowing employees to surf the Internet or shop online during their breaks, as long as they don't hog large amounts of bandwidth and thereby slow or harm Navy Operations. . . . Personal e-mail use is also acceptable, as are related on-line activities. Military personnel serving around the world are allowed broad use of Navy equipment.¹⁶³

Communication officers in the fleet have interpreted this policy to allow for limited personal use of government-provided Internet and e-mail. As one such officer noted, "One of the [Chief of Naval Operations'] initiatives is to provide a level of access to sailors of the [I]nternet for limited personal use. . . . Sending email to friends and family, banking, education and morale are authorized [uses] for sailors."¹⁶⁴

The Internet is not the only tool, though, that commanders use to maintain morale. They also use the ship's telephones and video-teleconferencing resources.¹⁶⁵ As previously discussed, all communications leaving the ship via telephone must use ship-based mechanisms. Even the commercially available lines must use ship transmitters to get their signals to relaying satellites. Cellular phone use within the "skin," or walls, of the ship is strictly prohibited, because the inside of the ship is considered to be a classified environment.¹⁶⁶ Regardless, cellular phones do not work in international waters, because of the lack of transmitter stations at sea.¹⁶⁷ As a result, Sailors and Marines can only use the telephone services provided aboard ship to make outside contact. Due to intermittent signals when in international waters and due to the high cost (fifty cents a minute) for a telephone call using the commercial line, in order to maintain regular contact with family or friends, the

¹⁶² See STAVRIDIS, *supra* note 5, at 80.

¹⁶³ Todd R. Weiss, *U.S. Navy Develops Acceptable-Use Policy for IT Equipment*, Dec. 22, 2004, COMPUTERWORLD, http://www.computerworld.com/s/article/98508/U.S._Navy_develops_acceptable_use_policy_for_IT_equipment.

¹⁶⁴ Premus, *supra* note 151.

¹⁶⁵ *Id.*; see also Malkasian, *supra* note 6.

¹⁶⁶ Johnson, *supra* note 9.

¹⁶⁷ *Id.*

servicemember is left to use either his government-provided e-mail account or use the government telephone line when morale calls are authorized.¹⁶⁸

While the use of government telephone lines are permitted occasionally for personal use, their use for personal matters is permitted less often than government e-mail due to the higher cost of making telephone calls while at sea. Typically, they are permitted on rare occasions when family emergencies or significant personal issues arise. In these circumstances, the Sailor or Marine may be allowed by his command to use ship telephones to contact family, friends or business associates.¹⁶⁹ For example, if the servicemember's child or spouse is seriously ill, or a spouse gives birth, then a commander may let the servicemember make a personal call.¹⁷⁰ This can include those service members who are pending divorce or other civil action as well. A commander may permit the servicemember to contact his civilian attorney or friends who are assisting to deal with issues as they arise.¹⁷¹ Just because the servicemember is deployed does not mean that the daily problems of home life stop, and as a result commanders permit the use of the communication systems available to deal with personal issues as they arise.¹⁷²

The personal use of video-teleconferencing equipment is permitted even less often than telephones. Possibly twice a deployment, servicemembers will be allowed to make personal use of video-teleconferencing equipment to contact family.¹⁷³ There will be designated times when this service is made available for personal use and these times will be advertised well in advance to both the deployed servicemembers and their family members back home.¹⁷⁴ Whether the personal use is of the ship's Internet, government-provided e-mail, or ship's telephones, monitoring is limited due to constraints on manpower and preferences among commanders.¹⁷⁵

C. The Monitoring Problem

The use of ship's Internet, government e-mail, and ship's telephones are all subject to monitoring by Information Assurance personnel aboard ship.¹⁷⁶ If a commander desired, he or she could have his or her Information Assurance

¹⁶⁸ *Id.*

¹⁶⁹ *Id.*

¹⁷⁰ *Id.*

¹⁷¹ Johnson, *supra* note 9.

¹⁷² See generally STAVRIDIS, *supra* note 5, at 80 (discussing the use of ship systems for personal use).

¹⁷³ Malkasian, *supra* note 6.

¹⁷⁴ *Id.*

¹⁷⁵ *Id.*

¹⁷⁶ *Id.*

personnel observe every Internet site visited by a servicemember in real time.¹⁷⁷ If he or she wished, the commander could potentially open and read every e-mail that a servicemember aboard ship sent or received, and could even have telephone calls made using ship telephones listened to by designated persons.¹⁷⁸ As a result, a commander could monitor every contact made by a servicemember using the ship's systems. He or she could even deny such services for personal use at all.¹⁷⁹ However, commanders aboard naval vessels typically do not go to these extremes for two reasons. First, commanders lack the resources to monitor every single personal contact made using these systems, and second, such a policy would seriously undermine morale.

Just as there is limited berthing and messing space aboard ship, there is also limited work space.¹⁸⁰ At any given time only a handful of Marines and Sailors work in the Information Assurance Section of the ship in order to maintain and monitor communication services.¹⁸¹ Instead of real-time system monitoring to guard against prohibited activities like accessing pornography sites on the Internet or revealing classified information via e-mail, Information Assurance Officers will typically write programs like firewalls and filters into the system that detect such unauthorized uses.¹⁸² Once an unauthorized site is accessed or a suspicious word or phrase is used in an e-mail, the Information Assurance Section will be alerted electronically.¹⁸³

This is how monitoring is done. Most commanders aboard ship do not allow Information Assurance personnel to monitor personal uses of the Internet or e-mail, unless alerted in this capacity, even though the technology exists to do so.¹⁸⁴ The reason for this is because it is unseemly for a computer technician to be looking over the shoulder, figuratively, at the personal e-mails or Internet transactions of other servicemembers, regardless of their rank.¹⁸⁵ For example, would a commander feel comfortable knowing that a communications officer is authorized to look at his executive officer or sergeant major's banking transactions made over the Internet aboard ship? The technology exists to allow this aboard ship, but due to inherent problems such monitoring would cause, it is typically not allowed.

¹⁷⁷ See Conrad, *supra* note 17, at 9-14 (discussing the means by which Information Assurance personnel can monitor the use of government communication systems).

¹⁷⁸ *Id.*

¹⁷⁹ See Memo from CIO, *supra* note 100.

¹⁸⁰ See generally WALLER, *supra* note 3, at 29 (describing cramped work space).

¹⁸¹ Malkasian, *supra* note 6.

¹⁸² Johnson, *supra* note 9.

¹⁸³ *Id.*

¹⁸⁴ Malkasian, *supra* note 6.

¹⁸⁵ Conrad, *supra* note 17, at 51.

Another issue deals with morale. If Sailors and Marines believed that their private banking transactions or educational assignments were being viewed by those working in the Information Assurance Section, they would be less likely to use the ship's Internet for these uses.¹⁸⁶ Likewise, they would be less likely to share intimate thoughts or feeling with loved ones over e-mail if they believed these messages would be read by other Marines or Sailors aboard ship.¹⁸⁷ If monitoring is unbridled, then the personal use of these systems would go away, and morale problems would arise. Without the ability to bank electronically, bills may not get paid, which turns into a problem for the command when creditors come calling.¹⁸⁸ Without the ability to contact loved ones and share personal thoughts, then loved ones may believe something is wrong with the servicemember and family ties will become strained, which eventually also becomes a command problem.¹⁸⁹ Regardless of the current DOD policy, the realities of life at sea demand that certain communications remain private and personal, and without unbridled government monitoring.

IV. WHY AN EXPECTATION OF PRIVACY STILL EXISTS ABOARD U.S. NAVAL VESSELS

The recent Memorandum from the DOD CIO attempts to eliminate any expectation of privacy in information passed using government communication systems, except for those few occasions when privileged communications may be exchanged.¹⁹⁰ It attempts to do this by dictating to the military departments the type of policy they will adopt and incorporate into use of their information systems.¹⁹¹ In a sense, the DOD is trying to nullify both prongs of the *Katz* expectation of privacy analysis, as applied to such systems, by requiring the military departments to adopt new log-on banners, enforce new notice and consent agreements, and implement new dictated policy.¹⁹² The logon banners and consent agreements are intended to eliminate any subjective beliefs of privacy by the individual user, while the policy itself is an attempt to eliminate any objective expectation of privacy in information passed using governmental information systems.¹⁹³ In most situations, this dictated policy may have the result of reducing or even possibly eliminating a Fourth Amendment protected expectation of privacy in information passed using these government systems, but it fails to address the realities of the use of such systems when deployed at sea.

¹⁸⁶ *See id.*

¹⁸⁷ *See id.*

¹⁸⁸ Johnson, *supra* note 9.

¹⁸⁹ *Id.*

¹⁹⁰ *See* Memo from CIO, *supra* note 100.

¹⁹¹ *Id.*

¹⁹² *Id.*

¹⁹³ *Id.*

A. The Gap between *Long* and the New DOD Policy

The conduct of system administrators in creating the honest belief in system users that personal information passed over military systems will be treated as private triggers a Fourth Amendment protected expectation of privacy. This is the general rule from *Long*.¹⁹⁴ The DOD CIO's attempts to eliminate the application of this rule to the military departments fails when applied to personal communications allowed by Sailors using ship-based communication systems while deployed. It fails for the simple reason that commanders and system administrators continue to implement policies (both in writing and verbally) that create in the mind of the average Sailor or Marine an expectation that their communications using these systems will remain private.¹⁹⁵

Even a mandated policy that attempts to eliminate the privacy expectation in government communications systems fails to have the effect of removing that expectation of privacy if the conduct of those in charge of implementing the policy is contrary to it.¹⁹⁶ In *Quon*, the Ninth Circuit recognized such a dilemma. The Ontario city government implemented a written policy regarding use of city-provided communication systems that was very similar to the current DOD policy. The policy applied to "[t]he use of City-owned computers and all associated equipment, software, programs, networks, Internet, e-mail and other systems operating on these computers. . . ."¹⁹⁷ The policy even went on to say that any use of these systems for personal benefit was a violation of policy, going even a step further than the current DOD Policy, which does allow limited personal use.¹⁹⁸ The city policy continued by adding, "The City of Ontario reserves the right to monitor and log all network activity . . . with or without notice. Users should have no expectation of privacy or confidentiality when using these resources. . . . Access to the Internet and e-mail system is not confidential."¹⁹⁹ The City even required its system users, to include Sergeant Quon, to sign an "Employee Acknowledgment" that used language from the general policy memorandum indicating the restrictive nature of the policy, just like the Department of Defense requires of servicemembers.²⁰⁰

Regardless of these restrictions, though, the Ninth Circuit found that Sergeant Quon had a Fourth Amendment protected expectation of privacy in

¹⁹⁴ *United States v. Long*, 64 M.J. 57, 64 (2006).

¹⁹⁵ Premus, *supra* note 151.

¹⁹⁶ *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 906-08 (9th Cir. 2008).

¹⁹⁷ *Id.* at 896.

¹⁹⁸ Compare *id.* (forbidding personal use of city-provided electronic systems) with Memo from CIO, *supra* note 100 (allowing limited personal use of Department of Defense electronic systems).

¹⁹⁹ *Quon*, 529 F.3d at 896.

²⁰⁰ *Id.*

personal text messages he sent using his city provided equipment.²⁰¹ The reason why the Ninth Circuit ruled in this manner was because of the conduct of local system administrators which gave rise to an honest and reasonably held expectation that personal text messages using the city system would be considered private.²⁰² In *Quon*, a Police Department Lieutenant told officers that he would not audit text messages, so long as the officers paid for any overages.²⁰³ Sergeant Quon had always paid for his overages when requested.²⁰⁴ In analyzing the stark differences between city policy and internal department implementation, the Ninth Circuit determined that “operational reality” would carry the day for determining Fourth Amendment protections.²⁰⁵ As a result, the court found that a protected expectation of privacy did exist in the personal text messages even though the city policy forbade any such personal use, and explicitly stated that any and all use would not be confidential.²⁰⁶

The CAAF’s analysis in *Long* followed a similar logic when it expressed, “the testimony of the network administrator is the most compelling evidence supporting the notion that Appellee had a subjective expectation of privacy.”²⁰⁷ The closer personal communications are to subjects concerning or similar to intimate family matters, the more likely a court will accord them Fourth Amendment protection.²⁰⁸ This is especially true if the communications being made are commonly known to system administrators as of the type which are normally considered intimate and private and the communications are still permitted.²⁰⁹

In the U.S. Navy, the use of government information systems for personal, private use while deployed aboard ship is common and accepted. Policy statements from fleet commanders, ship commanders and the Chief of Naval Operations allow and encourage limited personal use of government communication systems while deployed aboard ship.²¹⁰ It is common because

²⁰¹ *Id.* at 904.

²⁰² *Id.* at 907-08

²⁰³ *Id.*

²⁰⁴ *Quon*, 529 F.3d at 907-8.

²⁰⁵ *Id.*

²⁰⁶ *Id.*

²⁰⁷ *United States v. Long*, 64 M.J. 57, 63 (2006).

²⁰⁸ *See also United States v. Curry*, 46 M.J. 733, 739 (N-M. Ct. Crim. App. 1997) (discussing the distinction between the expectation of privacy in a military barracks vice a private family home).

²⁰⁹ *Compare id.* (discussing family privacy) *with Long*, 64 M.J. at 64 (discussing system administrator treatment of e-mail account as a privacy issue).

²¹⁰ *See* Policy Letter 06-02, Commanding Officer, 11th Marine Expeditionary Unit, subject: 11th MEU Internet and Unclassified/Classified LAN Usage Policy (6 Apr. 2006) (warning that there is no expectation of privacy in the use of government communication systems, but describing how personal e-mails sent using ship e-mail services will not be read by monitoring personnel); *see also* 13TH MARINE EXPEDITIONARY UNIT, ORDER 5500.1, DEPLOYED DIGITAL MEDIA POLICY para. 6 (13 Oct. 2008) (discussing how personal e-mails sent using ship e-mail services will not be read by

there is no other means by which a Sailor or Marine can routinely correspond with family and friends.²¹¹ The use of commercial carrier telephones is expensive and connectivity is sporadic due to the reliance on ship transmitters, which are needed for other more pressing operational matters.²¹² It is accepted because to deny the use of these services would severely hamper morale and would eventually result in increased tension between commanders, their staffs and the family members who are left behind.²¹³ If the individual Sailor or Marine cannot solve family or personal issues that arise back home on his own using government-provided systems while deployed, then how will he learn of the problems and then be permitted to take care of them? The only logical solution is either to allow the personal use or to increase the demand on the command for these matters.²¹⁴

A Pandora's Box of privacy issues arises in such an environment. If commanders allow personal use of these systems; are aware of the types of intimate communications that will be exchanged; and implement policies that limit the type of monitoring that can be done of these communications by use of firewalls and filters, due to the realized private nature of the communications, then privacy rights expressed in the decisions in *Quon* and *Long* will be triggered.²¹⁵ Once the conduct of ship's system administrators, to include commanders, create an expectation of privacy among Sailors and Marines in the communications they make using these systems, then Fourth Amendment protections will attach.²¹⁶ A blanket, boilerplate statement that "there is no expectation of privacy" in using the system will not counter the "operational reality" that an expectation of privacy does exist in practice.²¹⁷

monitoring personnel); Premus, *supra* note 151 (discussing Chief of Naval Operations initiatives that permit personal use of government e-mail); Conrad, *supra* note 17, at 24 (discussing each service's policy encouraging the personal use of government communication systems).

²¹¹ Malkasian, *supra* note 6.

²¹² *Id.*

²¹³ *Id.*

²¹⁴ *Id.*

²¹⁵ *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 906-08 (9th Cir. 2008); *see also* *United States v. Long*, 64 M.J. 57, 64 (2006).

²¹⁶ *Long*, 64 M.J. at 64.

²¹⁷ *Quon*, 529 F.3d at 896; *see also* *Watada v. Head*, 2008 U.S. Dist. LEXIS 88489 (W. Dist. Wash. Oct. 21, 2008). *Watada* provides an example of a successful collateral attack in federal court from a constitutional ruling in a military court-martial. It provides the framework for a potential collateral attack on a ruling by a military court, if it failed to apply the analysis in *Quon* in recognizing an expectation of privacy in certain permitted personal uses of DoD provided computer systems. In this case, the United States District Court for the Western District of Washington heard a habeas corpus petition from an accused pending court-martial. The issue was whether double jeopardy had attached after a military judge had declared a mistrial over the objection of the defense. After the military judge overruled the defense's motion to dismiss all charges, the accused petitioned the District Court claiming the U.S. Army had violated his Fifth Amendment right against double jeopardy. The district court stayed the trial until the case could be reviewed by the Army Court of Criminal Appeals (ACCA) and the CAAF. Both ACCA and CAAF ruled against the accused and

This application of the Fourth Amendment to personal communications using shipboard resources makes sense.²¹⁸ Would a commander really want a lance corporal working in the Information Assurance section viewing a staff sergeant's banking transactions? One argument to be made is that if the staff sergeant is concerned about this, then he should not use the ship-provided Internet to do his banking. This would make sense if the staff sergeant was home and banking on his office computer, or even if he chose to bank while deployed to a forward operating base when commercial Internet cafés are available, but on a ship his only option is to use ship resources.²¹⁹ Would a commander want a Sailor or Marine to avoid banking for possibly in excess of seventy days while at sea?²²⁰ Is it in the best interest of good order and discipline, if the Sailor or Marine is more concerned about financial issues than his duties because he cannot access the Internet for this use?²²¹ How about the use of the system to conduct educational research for classes completed for the AFLOAT Program? Does a commander want a lance corporal who may be in the same class as a monitored student viewing the research of that student?

How about intimate e-mails between spouses, fiancées, or close friends? After all, a ship is a very close community.²²² Would a commander want a lance corporal in the communications section to view these e-mails?²²³ Would a Sailor or Marine feel comfortable expressing his thoughts via e-mail to family or friends, banking on-line, or researching for graded papers, if he honestly believed that his use would be subject to unbridled monitoring and would not be private?²²⁴ Of course, the answer to all of these questions is no.

This is where a gap exists between the current DOD Policy and the "operational reality" of the use of ship-based electronic communications while deployed at sea. The policy wants to eliminate any and all expectation of privacy in communications made using government information systems, but it fails to recognize that in some circumstances there exists a need to maintain a

determined that the right of double jeopardy had not attached. *Id.* The accused then returned to the district court, which ruled in his favor on the double jeopardy issue. *Id.* The court cited several Ninth Circuit cases that supported the proposition that a district court could hear a collateral attack on a ruling by a military court on a habeas corpus petition. *Id.* at *25-26.

²¹⁸ Malkasian, *supra* note 6.

²¹⁹ *Id.*

²²⁰ See generally STAVRIDIS, *supra* note 5, at 116 (discussing the difficulty in spending seventy days at sea).

²²¹ *Id.*

²²² See generally WALLER, *supra* note 3, at 7 (detailing the closeness of personnel on ship and how gossip abounds).

²²³ 13TH MARINE EXPEDITIONARY UNIT, ORDER 5500.1, DEPLOYED DIGITAL MEDIA POLICY para. 6 (13 Oct. 2008).

²²⁴ See generally WALLER, *supra* note 3, at 7.

level of privacy.²²⁵ Regardless of the current policy, Navy and Marine commanders who embark upon ships for long deployments know the reality and allow a certain level of privacy to exist in personal communications.²²⁶ Due to this application of the policy, no matter how restrictive the DOD Policy may seem, the holdings in *Long* and *Quon* dictate that an expectation of privacy in electronic communications will still exist aboard a United States Naval vessel, so long as personal use is permitted.²²⁷

B. Why a Limited Expectation of Privacy Should Be Retained at Sea

A limited expectation of privacy in personal communications using ship based communication systems while deployed should be maintained for Sailors and Marines. In this electronic age where so much contact with the outside world is done using computers or satellites, it is unrealistic to deny a Sailor or Marine a limited level of personal, private communication using the only system available to him or her while deployed at sea.²²⁸ It is especially unrealistic when such personal, private communications are at times required by superiors when personal problems arise.²²⁹ Allowing the use of ship systems in this capacity solves more problems than it creates. The use maintains morale among both the servicemember and his family members by keeping them routinely in touch.²³⁰ It saves servicemembers money by reducing the need for expensive, unreliable commercially provided telephone lines.²³¹ It helps commanders maintain good order and discipline by allowing servicemembers the ability to solve personal problems that may arise during a deployment on their own, without command intervention.²³² The problem it creates is that users could potentially access unauthorized Internet sites, conduct criminal activity using the provided system, or pass classified information either intentionally or negligently.²³³ As discussed, though, mechanisms exist to thwart these abuses.

The best mechanism is the use of system firewalls.²³⁴ Firewalls prevent users from accessing certain prohibited sites.²³⁵ They also limit the use of

²²⁵ Malkasian, *supra* note 6.

²²⁶ *Id.*; see also Premus, *supra* note 151.

²²⁷ *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 906-08 (9th Cir. 2008); see also *United States v. Long*, 64 M.J. 57, 64 (2006).

²²⁸ Malkasian, *supra* note 6.

²²⁹ *Id.*

²³⁰ See generally STAVRIDIS, *supra* note 5, at 116 (discussing the importance of family contacts while deployed).

²³¹ Malkasian, *supra* note 6.

²³² *Id.*

²³³ See Conrad, *supra* note 17, at 50 (recommending constant monitoring, with checks, for these risks).

²³⁴ Malkasian, *supra* note 6.

permitted sites during peak hours when limited bandwidth is at a premium.²³⁶ By the extensive use of firewalls, most pornography sites or other impermissible sites can be blocked.²³⁷ In addition, Information Assurance personnel will be alerted when a user attempts to access a prohibited site.²³⁸ Since the computer and account used to access the site belongs to the government, the user can then be immediately denied continued access and the computer can be confiscated and re-assigned.²³⁹ If the need for evidence arises for later court-martial, the alert on the firewall can form the basis for probable cause for a later search authorization.²⁴⁰

The next best mechanism is the use of system filters.²⁴¹ These filters cause alerts to be given to the Information Assurance personnel when questionable words or phrases are used in e-mails.²⁴² For example, if the word “Afghanistan” is used and this word has been added to the filter, the communications section will be alerted that the word was used in an e-mail sent by a certain user.²⁴³ The filter will not open the e-mail.²⁴⁴ If the word had been used while at sea on a deployment headed to Afghanistan there could exist the potential that classified information may have been passed or attempted to be passed. This too could form the basis for a probable cause search of the e-mail.²⁴⁵ Whether the e-mail would be opened or not would be up to the commander to decide.²⁴⁶ It is not a difficult process to get a search authorization. The commander must simply review evidence that gives him or her a reasonable belief that a crime has been committed and the requested search would bring about evidence of that crime.²⁴⁷

This is where the DOD, in promulgating its new policy, overreacted to *Long*. The current policy, in reaction to *Long*, has tried to eliminate any and all expectation of privacy in the personal use of government-provided information

²³⁵ *Id.*; see also GRALLA, *supra* note 152, at 329 (defining firewall as “[a] hardware or hardware/software combination that protects computers on a network from being attacked by hackers or snoopers”).

²³⁶ Premus, *supra* note 151.

²³⁷ Malkasian, *supra* note 6.

²³⁸ *Id.*

²³⁹ 13TH MARINE EXPEDITIONARY UNIT, ORDER 5500.1, DEPLOYED DIGITAL MEDIA POLICY para. 6 (13 Oct. 2008).

²⁴⁰ See MCM, *supra* note 77, MIL. R. EVID. 315.

²⁴¹ Conrad, *supra* note 17, at 9-15.

²⁴² Malkasian, *supra* note 6 (describing a filter as a “flag”); see also GRALLA, *supra* note 152, at 279 (defining a filter as “a screening router [that examines] . . . every packet of data traveling between the Internet and the . . . network”).

²⁴³ Johnson, *supra* note 9.

²⁴⁴ *Id.*

²⁴⁵ See MCM, *supra* note 77, MIL. R. EVID. 315.

²⁴⁶ *Id.*

²⁴⁷ *Id.*

systems to avoid the possibility that evidence may be excluded at trial if a subsequent search done without a valid search authorization reveals criminal misconduct.²⁴⁸ This was an overreaction. In *Long*, an investigator had a suspicion that LCpl Long was engaged in criminal misconduct.²⁴⁹ He had reason to believe that her government e-mail account could reveal evidence of such misconduct.²⁵⁰ He then side-stepped the requirements of MRE 315 for probable cause searches by failing to get a search authorization from the controlling commander in order to search the account.²⁵¹ If he would have followed the correct procedure, then it is probable that the e-mails would have been seized legally and her conviction upheld.²⁵² A search of a user's account, if not conducted for the purposes of obtaining evidence for court-martial, is really of no legal effect.²⁵³ If it is done just for security purposes due to the user misusing the system then the user can simply be denied access.²⁵⁴ It is when an attempt is made to collect evidence that Fourth Amendment issues arise in the military.²⁵⁵

Even so, the technology available in today's firewalls and filters provides, in most cases, the necessary information to develop probable cause for a search authorization. Even if an expectation of privacy exists, once a misuse is alerted on the firewall or through a filter, probable cause will most likely exist, from the information provided via the alert, for a valid Fourth Amendment search. It is better that users be made aware of this type of monitoring to reduce privacy expectations, rather than to attempt to eliminate privacy altogether especially when the privacy interest involved concerns Sailors and Marines deployed at sea who have no other option but to use these systems.²⁵⁶

The bottom line is that the current DOD policy on the use of government information systems is impractical and unrealistic in application to sea-based Sailors and Marines. It is too broad and does not account for the available, effective monitoring options to avoid what it claims is its main purpose – breaches of communications security.²⁵⁷

²⁴⁸ Memo from CIO, *supra* note 100.

²⁴⁹ *United States v. Long*, 64 M.J. 57, 59-60 (2006).

²⁵⁰ *Id.*

²⁵¹ *Id.*

²⁵² *Id.* at 64.

²⁵³ *Id.*

²⁵⁴ 13TH MARINE EXPEDITIONARY UNIT, ORDER 5500.1, DEPLOYED DIGITAL MEDIA POLICY para. 6 (13 Oct. 2008).

²⁵⁵ MCM, *supra* note 77, MIL. R. EVID. 315.

²⁵⁶ Malkasian, *supra* note 6.

²⁵⁷ Memo from CIO, *supra* note 100.

V. CONCLUSION

A limited expectation of privacy currently exists in personal communications made using ship-based electronic systems. Although it has made an attempt, the current DOD policy has not altogether eliminated this Fourth Amendment protection because, regardless of written policy, courts have routinely protected personal communications through government systems if system administrators create a reasonable inference that personal communications using these systems will be considered private.²⁵⁸ In the U.S. Navy, commanders and system administrators routinely allow the use of ship systems for personal communications.²⁵⁹ Their limited monitoring policies create an inference that certain types of these personal communications are private and confidential. As a result, Fourth Amendment protections attach to some types of these communications, like personal banking, e-mails sent to family and friends, and educational research. This continued expectation of privacy is not a bad thing and it should not be eliminated. Ship-based systems are the only means of communication available for Sailors and Marines to conduct personal matters while deployed aboard ship.²⁶⁰ A minimal level of confidentiality creates confidence in service members that their personal business will remain their own, even when using ship-based systems. This confidence lessens the impact of deployments on the command structure. The more able servicemembers are to deal with personal problems on their own, the less the command structure will be drawn away from operational concerns to deal with personal issues between deployed servicemembers and their families.

The concern over misuse can be nullified by using firewalls and filters. Firewalls and filters alert Information Assurance personnel when an impermissible Internet site has been visited or suspect language has been sent in an e-mail.²⁶¹ These alerts can form the basis for a legitimate probable cause search.²⁶² As a result, operational security and personal privacy can co-exist in a sea-based environment without the need for stripping away the limited Fourth Amendment expectation of privacy individual Sailors and Marines enjoy in these systems. In the end, an expectation of privacy in ship-based communication systems is an operational reality that is desired, needed, and not going away any time soon.

²⁵⁸ *United States v. Long*, 64 M.J. 57, 64 (2006).

²⁵⁹ *See Premus, supra* note 151.

²⁶⁰ *See Malkasian, supra* note 6.

²⁶¹ *See Johnson, supra* note 11.

²⁶² *See MCM, supra* note 77, MIL. R. EVID. 315.

FEDERAL COURT OR MILITARY COMMISSION: THE LEGAL DILEMMA POSED BY THOSE CHARGED WITH TERRORIST VIOLENCE

Colonel James P. Terry (Ret.)¹

I. INTRODUCTION

The November 2009 decision announced by Attorney General Eric Holder to try Khalid Sheikh Mohammed (“KSM”) and four other alleged terrorists² in federal court in New York has raised a number of important and timely questions concerning the nature of law of war violations and the challenges raised to their successful prosecution in federal court. Following al Qaeda’s September 11, 2001 attack, the United States captured or apprehended a number of “high value” detainees who were believed to have committed or conspired to commit terrorist acts against the United States, its military forces, or its citizens. These acts also constituted violations of federal criminal law under Title 18, United States Code.

Where prosecution in federal court is contemplated, however, the Fourth, Fifth and Sixth Amendments addressing the right to privacy, the right to due process in criminal investigations, and the right of confrontation, respectively, often collide with the need to ensure the nation’s security. The Fourth Amendment, for example, requires specificity on the part of federal agents in obtaining judicial authorization to physically invade the privacy of individuals. In that regard, the Fourth Amendment was designed to preclude overreaching in investigations of criminal enterprises. The forefathers simply did not contemplate the investigation and prosecution of terrorist threats to our nation.

The refinement of Fifth Amendment standards in the context of national security has developed unevenly as well. Statements obtained from detainees such as KSM through harsh interrogation as a result of perceived extreme necessity have led to the development of other evidence that could be

¹ Colonel James P. Terry, USMC (Ret.) serves as Chairman of the Board of Veterans Appeals, having previously served as Principal Deputy Assistant Secretary and Deputy Assistant Secretary of State, and as Legal Counsel to the Chairman of the Joint Chiefs of Staff. He is widely published in the area of national security law. The views expressed are solely those of the author.

² The remaining four are Walid Muhammad Salih Mubarak Bin’Attash, Ramzi Binalshibh, Ali Abdul Aziz Ali, and Mustafa Ahmed Adam al Hawsawi.

the subject of successful constitutional challenge. Congress recognized the obvious conflict between normal federal prosecutions and the special requirements in prosecuting national security violations by al Qaeda, and, accordingly, passed the Military Commissions Act of 2006.³

This article addresses the actions taken by the Congress to address the dichotomy between national security cases and normal federal prosecutions, the legislative standards developed to ensure the successful prosecution of national security violations in military commissions, and the constitutional concerns that are likely to arise in the five federal prosecutions in New York. These concerns include the detainees' right to counsel and to a speedy trial, the problem of coerced statements and their fruit, and limitations upon the admissibility of hearsay and classified evidence in criminal cases.

II. NATIONAL SECURITY VERSUS PROTECTION OF PERSONAL LIBERTY

There will always be tension between the requirements of national security and the protection of personal liberties found in the Bill of Rights. While these amendments were never intended to provide for the nation's security, their application, especially when Fourth and Fifth Amendment values are implicated, has differed in times of national crisis when compared to times of relative peace. This is clearly reflected in the probable cause requirements in normal criminal investigations when compared to national security investigations. In solely criminal investigations, the probable cause requirement is "a fair probability that contraband or evidence of a crime will be found in a particular place."⁴ Conversely, the probable cause standard for national security investigations is an external threat to the security of the nation.⁵

In the days immediately following the 9/11 attacks, the Bush Administration issued the Military Order of November 13, 2001, which established military commissions to address detention and trial of non-citizens held in the war on terrorism.⁶ It was contemplated that these unlawful combatants would be tried by military commission outside the United States.⁷ In *Rasul v. Bush*,⁸ however, the Supreme Court held that U.S. federal courts do have jurisdiction to hear the *habeas corpus* petitions of these detainees.

³ Pub. L. No. 109-366, 120 Stat. 2600 (2006).

⁴ *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

⁵ See M. E. Bowman, *National Security and the Fourth and Fifth Amendments*, in John N. Moore & Robert F. Turner, eds., *NATIONAL SECURITY LAW* 1059 (2005).

⁶ Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism § 1(a), 66 Fed. Reg. 57,833 (Nov. 16, 2001).

⁷ See James P. Terry, *Habeas Corpus and the Detention of Enemy Combatants in the Global War on Terror*, 48 *JOINT FORCE Q.* 14 (2008).

⁸ *Rasul v. Bush*, 542 U.S. 466 (2004).

Following the submission of numerous petitions for habeas corpus in the U.S. District Court for the District of Columbia, the Congress in 2005 revoked federal district court jurisdiction over these petitions through enactment of the Detainee Treatment Act (“DTA”).⁹ The DTA provided that the U.S. Court of Appeals for the District of Columbia would hear all appeals from final decisions of military commissions. In 2006, the Supreme Court decided *Hamdan v. Rumsfeld*,¹⁰ reversing a D.C. Circuit decision upholding military commissions. *Hamdan* provided that although the Congress had approved military commissions, their procedures must be as similar as possible to military court-martial proceedings.¹¹ The Supreme Court declared that it was immaterial whether the Geneva Conventions of 1949, and specifically Common Article 3 to those Conventions, provided rights enforceable on behalf of detainees in federal district court. By incorporating the laws of war into the Uniform Code of Military Justice (“UCMJ”) at Article 21, Congress brought the Geneva Conventions within the body of law to be applied at courts-martial and in military commissions.¹²

Shortly after his election, President Barack Obama ordered the detention facility at Guantanamo Bay closed no later than January 22, 2010.¹³ Under this Executive Order, the Attorney General, in coordination with other Administration Officials,¹⁴ was required to assess the status of each detainee and determine whether he should remain in U.S. custody, be transferred to a third country, or be prosecuted for criminal offenses.¹⁵ When this review was completed, the Attorney General and Secretary of Defense jointly announced on November 13, 2009 that ten detainees, all of whom previously had been charged before military commissions, would be tried.¹⁶ Five, previously identified herein, would be tried in the U.S. District Court for the Southern District of New York, and the remaining five would be tried by military commission.¹⁷

⁹ Detainee Treatment Act of 2005, Pub. L. No. 109-148, tit. X, 119 Stat. 2680 (2005).

¹⁰ *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006), *rev’d* 415 F.3d 33 (D.C. Cir. 2005).

¹¹ The procedural rules for court martial proceedings are set forth in the Uniform Code of Military Justice, 10 U.S.C. §§ 801-946.

¹² *Hamdan*, 548 U.S. at 627-28.

¹³ Exec. Order No. 13,492, 74 Fed. Reg. 4897 (Jan. 22, 2009) [hereinafter Executive Order].

¹⁴ *Id.* § 4. The Attorney General is required to coordinate with the Secretary of Defense, Secretary of State, Secretary of Homeland Security, Director of National Intelligence, and the Chairman, Joint Chiefs of Staff.

¹⁵ *Id.* § 4(c).

¹⁶ Press Release, Departments of Justice and Defense Announce Forum Decisions for Ten Guantanamo Bay Detainees (Nov. 13, 2009), <http://www.justice.gov/opa/pr/2009/November/09-ag-1224.html> [hereinafter Press Release].

¹⁷ *Id.*

III. EXECUTIVE AUTHORITY TO ESTABLISH MILITARY COMMISSIONS

The President's authority to convene military commissions to try criminal violations by those involved in armed conflict flows from his Commander in Chief powers under the Constitution.¹⁸ Under Title 10, U.S. Code, the President may convene such bodies to try offenses against the laws of war.¹⁹ Unlike the court-martial process established by the UCMJ to maintain discipline and order among U.S. forces, the military commission is directed at enemy combatants as a means of deterring and punishing violations of the law of armed conflict.²⁰ When President Bush first signed a Military Order establishing commissions to try terrorism suspects in 2001, the process had not been used since World War II.²¹ As courts established under the President's Article I executive authority, as opposed to the Article III federal judiciary, military commissions are not subject to the same constitutional requirements applied in federal courts.²²

The Supreme Court further determined in *Hamdan* that, although Common Article 3 of the Geneva Conventions of 1949 "tolerates a great degree of flexibility in trying individuals captured during armed conflict,"²³ and was "crafted to accommodate a wide variety of legal systems,"²⁴ the procedures established in Military Commission Order Number 1²⁵ to effectuate the President's Military Order of November 13, 2001, did not meet even this low threshold.²⁶

To effect the mandate in *Hamdan*, Congress then enacted the Military Commissions Act of 2006 ("MCA")²⁷ which authorized military commissions, and established procedural rules that are modeled after, but differ in several

¹⁸ U.S. CONST. Art. II, § 2, cl. 1; see James P. Terry, *The President as Commander in Chief*, 7 AVE MARIA L. REV. 391 (2009) (arguing for broad interpretation of Commander in Chief powers).

¹⁹ See UCMJ art. 21 (2008). Statutory offenses for which military commissions may be convened are limited to aiding the enemy, UCMJ art. 104 (2008), and spying, UCMJ art. 106 (2008). These offenses are explicitly included in the MCA.

²⁰ See WILLIAM WINTHROP, MILITARY LAW AND PRECEDENTS 831 (2d ed. 1920) (describing the distinction between courts-martial and military commissions).

²¹ Military Order No. 1, 2001, Nov. 13, 2001, published as Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism § 1(a), 66 Fed. Reg. 57,833 (Nov. 16, 2001). The United States first used military commissions during the occupation of Mexico in 1847, and made heavy use of them in the Civil War and in the Philippine Insurrection.

²² See *Ex Parte Quirin*, 317 U.S. 1, 38 (1942); *Ex Parte Milligan*, 71 U.S. (4 Wall) 2, 123 (1866) (noting a service member "surrenders his right to be tried by the civil courts").

²³ *Hamdan v. Rumsfeld*, 548 U.S. 557, 632 (2006).

²⁴ *Id.*

²⁵ Reprinted at 41 I.L.M. 725, Mar. 21, 2002.

²⁶ *Hamdan*, 548 U.S. at 632.

²⁷ Pub. L. No. 109-366, 120 Stat. 2600 (2006).

significant ways from, the UCMJ. The MCA created Chapter 47a of Title 10, U.S. Code, declaring that it is “based upon the procedures for trial by general courts-martial under [the UCMJ].”²⁸ It then exempted the new military commissions from UCMJ requirements under Article 10 (speedy trial), Article 31 (self-incrimination warnings), and Article 32 (right to a formal pretrial investigation).²⁹

These legislative efforts were successfully challenged, at least in part, in 2008 in *Boumediene v. Bush*, in which the Supreme Court held that *habeas corpus* extends to non-citizens detained at Guantanamo Bay and that these non-citizens could seek *habeas* review of their status.³⁰ *Boumediene* struck section 7 of the MCA as it relates to the right of detainees in Guantanamo Bay to challenge their detention in federal court. The extent to which Fourth, Fifth and Sixth Amendment protections extend to these non-citizens has not yet been determined, however.³¹ Many believe these issues will be addressed in *Kiyemba v. Obama*,³² scheduled for Supreme Court argument in spring 2010.

IV. CONGRESS’ ROLE IN THE MILITARY COMMISSION PROCESS

Article I, section 8 of the Constitution grants significant war powers to Congress. Its power to “define and punish . . . offenses against the laws of nations”³³ provides a basis for Congress to establish a statutory framework, such as that set forth in the MCA, for trying and punishing unlawful enemy combatants for violations of the law of war and other hostile acts in support of terrorism.³⁴ This view was confirmed by former President Bush’s support for the MCA following the Supreme Court’s decision in *Hamdan v. Rumsfeld*.³⁵ Furthermore, the power “[t]o make rules for the government and regulation of the land and naval forces”³⁶ gives Congress the recognized authority to establish standards for the detention, interrogation, and transfer to foreign nations. This is precisely what the Congress did in passing the Detainee Treatment Act of 2005,³⁷ which addresses the treatment of alien detainees held in the custody of the Department of Defense.

²⁸ UCMJ art. 148a (2008).

²⁹ *Id.* § 4 (amending UCMJ Art. 21).

³⁰ *Boumediene v. Bush*, 553 U.S. 723 (2008); see also James P. Terry, *Habeas Corpus and the War on Terror*, in John Norton Moore & Robert F. Turner, eds., *LEGAL ISSUES IN THE STRUGGLE AGAINST TERROR* (2010) (in press).

³¹ See Michael John Garcia, *Boumediene v. Bush: Guantanamo Detainees’ Right to Habeas Corpus*, CRS Report RL34536 (2008).

³² *Kiyemba v. Obama*, 130 S. Ct. 458 (2009).

³³ U.S. CONST. Art. I, § 8, cl. 10.

³⁴ Pub. L. No. 109-366, 120 Stat. 2600 (2006).

³⁵ 548 U.S. 557 (2006).

³⁶ U.S. CONST. Art. I, § 8, cl. 14.

³⁷ Pub. L. No. 109-148, 119 Stat. 2680 (2005).

While the President and Congress share responsibility for detainee matters, the detention and prosecution of unlawful combatants rests solely with the Executive. Early in the present conflict, the Congress passed Senate Joint Resolution (“SJR”) 23,³⁸ which recognizes that “the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States.”³⁹ Additionally, the resolution specifically authorizes the President

to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist acts that occurred on September 11, 2001, or harbored such organizations or persons, *in order to prevent any future acts of international terrorism against the United States* by such nations, organizations or persons.⁴⁰

Thus, Congress in SJR 23 has specifically endorsed not only the use of appropriate military force, but also the included authority to detain and try enemy combatants to prevent them from conducting further hostilities against this nation.

Under the provisions of the MCA, as amended in 2009,⁴¹ the Secretary of Defense has established regulations for the conduct of commission proceedings. The jurisdiction of any military commission is limited to a time of war. Only offenses recognized under the law of war or designated by statute may be tried by military commission. The MCA further provides that only aliens may be tried.⁴²

V. PROCEDURES BEFORE MILITARY COMMISSIONS VERSUS FEDERAL DISTRICT COURT

The five detainees currently awaiting military commission proceedings in Guantanamo Bay⁴³ will face proceedings that differ greatly from those in

³⁸ Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).

³⁹ *Id.* at pmbl.

⁴⁰ *Id.* § 2(a).

⁴¹ National Defense Authorization Act for Fiscal Year 2010, Pub. L. No. 111-84, tit. XVIII, 123 Stat. 2574 (2009).

⁴² *Id.*

⁴³ These include Omar Khadr, a Canadian citizen captured as a teenager and charged before a military commission for allegedly throwing a hand grenade that killed a U.S. medic in Afghanistan; abd al-Rahim al-Nashiri, whose military commission charges related to the October 2000 attack on the USS Cole (DDG 67) were previously withdrawn in February 2009; Ahmed Mohammed Ahmed

federal district court. For example, the Fifth Amendment's requirement that no prosecution for a capital or otherwise infamous crime can proceed unless on presentment or indictment of a grand jury has been specifically excepted from military commission proceedings.⁴⁴ Similarly, the requirements concerning trial by jury in the Sixth Amendment have been found to be inapplicable to trials before military commissions.⁴⁵ Due process requirements also differ. Fifth Amendment due process protections in military commissions and courts are subject to the Congress' "plenary control over rights, duties, and responsibilities in the framework of the Military Establishment, including regulations, procedures and remedies related to military discipline."⁴⁶ In *Weiss*, the Supreme Court upheld a narrowed interpretation of Fifth Amendment due process in the context of military criminal proceedings.⁴⁷

The military commissions authorized by the MCA, in fact, afford the detainees fewer procedural protections overall than would be available to defendants in either a military court-martial or in federal court.⁴⁸ A careful review of procedural and substantive rights in a military commission versus a federal district court may prove helpful.

a. Assistance of Counsel

The right to assistance of counsel in any criminal proceeding is considered the most basic of U.S. constitutional rights. The Sixth Amendment makes clear that every criminal defendant has the right "to have the Assistance of Counsel for his defence."⁴⁹ The Supreme Court has ruled that it is not just the

Haza al Darbi, who is accused of participating in an al Qaeda plot to blow up oil tankers in the Straits of Hormuz; and two other detainees about whom no further information has been provided.

⁴⁴ See U.S. CONST. amend. V ("No person shall be held to answer for a capital, or otherwise infamous crime, unless on presentment or indictment of a Grand Jury, *except* in cases arising in the land or naval forces, . . .") (emphasis added).

⁴⁵ See, e.g., *Ex Parte Quirin*, 317 U.S. 1, 40 (1942) ("[W]e must conclude that § 2 of Article III and the Fifth and Sixth Amendments cannot be taken to have extended the right to demand a jury to trials by military commission, or to have required that offenses against the law of war not triable by jury at common law be tried only in the civil courts."); *Welch v. McDonald*, 340 U.S. 122, 127 (1950) ("The right to trial by jury guaranteed by the Sixth Amendment is not applicable to trials by courts-martial or by military commissions.").

⁴⁶ *Weiss v. United States*, 510 U.S. 163, 177 (1994) (quoting *Chappell v. Wallace*, 462 U.S. 296, 301 (1983)).

⁴⁷ See also *Chappell*, 462 U.S. at 301.

⁴⁸ See generally *The Military Commissions Act of 2006: Analysis of Procedural Rules and Comparison with Previous DoD Rules and the Uniform Code of Military Justice*, CRS Report RL 33688 (2007).

⁴⁹ U.S. CONST. amend. VI.

assistance of counsel, but the *effective* assistance of counsel that is required.⁵⁰ In federal criminal courts, this right is effected through Rule 44 of the Federal Rules of Criminal Procedure.⁵¹ Under this Rule, a defendant who is unable to afford counsel will have one appointed to represent him at every stage of the proceedings unless he waives that right.⁵²

The rule concerning the right to counsel before military commissions is similar.⁵³ Rule 506 of the Rules for Military Commissions provides a detainee charged with criminal offenses with a detailed military defense counsel at no cost to him. The detainee may also request a specific military defense counsel, and if reasonably available, that counsel will be provided.⁵⁴ The detained unlawful combatant may also retain a civilian counsel, but at no cost to the government. Non-military counsel must also have U.S. citizenship and a security clearance, in light of the sensitivity of the charges in this forum.⁵⁵ As in the case of a federal court proceeding, the defendant before a military commission may waive his right to attorney representation and represent himself.⁵⁶

b. Right Against Self-Incrimination

The Fifth Amendment to the Constitution makes clear that “[n]o person . . . shall be compelled in any criminal case to be a witness against himself . . .”⁵⁷ The Supreme Court has clearly articulated the self-incrimination clause rationale for excluding coerced statements in federal courts.⁵⁸ The Supreme Court has also recognized a Fourteenth Amendment due process rationale for excluding statements in federal courts where they are the product of coercive interrogation methods.⁵⁹ As a general rule, federal courts do not admit statements of a defendant in criminal proceedings unless the law enforcement or

⁵⁰ Strickland v. Washington, 466 U.S. 668, 686 (1984) (quoting McMann v. Richardson, 397 U.S. 759, 771 n.14 (1970)); see also Glasser v. United States, 315 U.S. 60, 70 (1942); Powell v. Alabama, 287 U.S. 45, 71-72 (1932).

⁵¹ Fed. R. Crim. P. 44.

⁵² Fed. R. Crim. P. 44(a).

⁵³ See 10 U.S.C. §§ 949a, 949c (as amended by Pub. L. No. 111-84 § 1802 (2009)).

⁵⁴ 10 U.S.C. § 949c (as amended by Pub. L. No. 11-84 § 1802 (2009)).

⁵⁵ *Id.* § 949c(b).

⁵⁶ 10 U.S.C. § 949a(b)(2)(D) (as amended by Pub. L. No. 11-84 § 1802 (2009)).

⁵⁷ U.S. CONST. amend. V.

⁵⁸ Miranda v. Arizona, 384 U.S. 436, 444-45 (1966); Bram v. United States, 168 U.S. 532, 542 (1887).

⁵⁹ Dickerson v. United States, 530 U.S. 428, 434 (2000); Brown v. Mississippi, 297 U.S. 278, 285-87 (1936).

other federal official taking the statement issued *Miranda* warnings before the statements were made.⁶⁰

There are two exceptions to the *Miranda* rule possibly germane to the federal court detainee proceedings in New York. The first is the public safety exception addressed in *New York v. Quarles*.⁶¹ In *Quarles*, however, the time-sensitive nature of the question, “Where is the gun?” was key.⁶² In certain of the detainee cases, it may not be so relevant. The second possible *Miranda* exception applicable to certain detainees relates to foreign interrogations and the fact that courts have not extended *Miranda* to questioning by foreign officials overseas,⁶³ unless they are working jointly with U.S. officials or the interrogation would “shock the judicial conscience.”⁶⁴

The Congress has taken a very different view of *Miranda* for detainees held outside the United States and tried by military commission. In the 2009 amendments to the 2006 MCA,⁶⁵ Congress barred enemy combatants in military custody held outside the United States from being read *Miranda* warnings, absent a court order.⁶⁶ Though *Miranda* does not apply, detainees tried by military commission do have a statutory right against self-incrimination. Under the 2009 amendments to the MCA, all detainee statements obtained through torture, or “cruel, inhuman or degrading treatment” are inadmissible in military commission proceedings, regardless of when taken.⁶⁷ Similarly, a detainee before a military commission may not be required to testify against himself.⁶⁸ The 2009 amendments to the MCA do provide an opportunity to consider incriminating statements of detainees where the commission is satisfied the

⁶⁰ See *Miranda*, 384 U.S. at 467-71. The *Miranda* requirement applies any time federal officials have a suspect in custody. The warning typically begins with “You have a right to remain silent . . .” before the statement is taken. In the context of terrorist suspects’ statements, at least one court has held that *Miranda* applies in Article III courts even if the questioning took place outside of the United States. See *United States v. Bin Laden*, 132 F. Supp. 2d 168, 183 (S.D.N.Y. 2001).

⁶¹ 467 U.S. 649 (1984).

⁶² *Id.* at 657-58 (reasoning that requiring police to determine whether to take the time to give *Miranda* warnings “in a matter of seconds” was impracticable under the circumstances).

⁶³ *United States v. Yousef*, 327 F.3d 56, 145-46 (2d Cir. 2003) (failing to apply the “joint venture” doctrine, under which statements elicited during overseas interrogation by foreign police in the absence of *Miranda* warnings must be suppressed whenever United States law enforcement agents actively participate in questioning conducted by foreign authorities), *cert denied*, 540 U.S. 933 (2003).

⁶⁴ *Id.* at 146. See also *United States v. Abu Ali*, 528 F.3d 210, 232-34 (4th Cir. 2008). In *Abu Ali*, a case involving a defendant who had been arrested and questioned by Saudi officials for assisting terrorists in an attack, the Fourth Circuit found that statements made to the Saudi interrogators, despite a lack of *Miranda* warnings, were voluntary.

⁶⁵ *Supra* note 38.

⁶⁶ Pub. L. No. 111-84 §1040, 123 Stat. 2190 (2009).

⁶⁷ 10 U.S.C. § 948r(a) (as amended by Pub. L. No. 111-84 § 1802 (2009)).

⁶⁸ *Id.* § 948r(b).

statements are trustworthy. Specifically, the amendments provide that for statements to be admissible, the military commission must determine:

(1) that the totality of the circumstances renders the statement reliable and possessing sufficient probative value; and

(2) that (A) the statement was made incident to lawful conduct during military operations at the point of capture or during closely related active combat engagement, and the interests of justice would best be served by admission of the statement into evidence, or (B) the statement was voluntarily given.⁶⁹

c. Evidentiary Issues

A critical prosecution issue either in federal court or before a military commission is hearsay evidence. Hearsay is a prior out-of-court statement offered at trial to prove the truth of the matter asserted. This is especially significant in the context of a terrorist trial where crucial witnesses detained by foreign governments may be unavailable to come to the United States to testify, or the U.S. or a foreign government may be unwilling to make intelligence operatives available for the proceeding. Both federal courts and military commissions have established procedural rules governing the admission of evidence.

Under the Federal Rules of Evidence, hearsay is generally inadmissible unless an exception can be asserted.⁷⁰ Exceptions to the hearsay rule exist where the context in which the statement was made or the nature of the content of the statement gives it greater inherent trustworthiness than other out of court statements. Some examples include statements of a self-incriminating nature, records of a regularly conducted activity, excited utterances made in response to a startling event, or certain statements by a person who is deceased or was facing impending death.⁷¹ Another exception permits the introduction of

⁶⁹ *Id.* § 948r(c). To determine voluntariness, the military commission must consider the totality of the circumstances, including:

(1) The details of the statement, accounting for the circumstances of the conduct of military and intelligence operations during hostilities; (2) The characteristics of the accused, such as military training, age and education level; and (3) The lapse of time, change of place, or change in identity of the questioners between the statement sought to be admitted and any prior questioning of the accused.

Id. § 948r(d).

⁷⁰ Fed. R. Evid. 802.

⁷¹ Fed. R. Evid. 801(d), 803.

evidence, over hearsay objection, when the statement has an “equivalent circumstantial guarantee of trustworthiness.”⁷² Some statements that federal courts have recognized under this exception, which will be critical to the proceedings in New York, are those contained within the files of foreign intelligence authorities.⁷³

Also exempted from the federal hearsay rule are statements made by co-conspirators in furtherance of the conspiracy.⁷⁴ These statements are not technically considered hearsay. While the conspiracy must be proved before this rule can be applied, the same hearsay statements may be used to prove the existence of the conspiracy, but only if the hearsay is corroborated by other reliable evidence.

The evidentiary rules under the Military Commission Rules of Evidence (“MCRE”), as amended in 2009, are far more flexible, and even permissive. Under the MCRE, hearsay is not excluded in two situations. Hearsay is admitted if it would otherwise be admitted under the Military Rules of Evidence applicable in general courts-martial, or if the proponent of the evidence makes known to the adverse party 30 days in advance the intention to offer the evidence, as well as the circumstances under which it was taken.⁷⁵ These particulars should include the time, place and conditions under which the statement was taken.⁷⁶ The evidence would only be excluded if the totality of the circumstances under which it was taken shows the statement to be unreliable.⁷⁷

d. Right to a Speedy Trial in Criminal Prosecutions

The Sixth Amendment guarantees the right to a speedy trial to all criminal defendants.⁷⁸ The right applies to prosecutions in both federal and state courts, as the Supreme Court has found the right to be one of the “fundamental” constitutional rights the Fourteenth Amendment applied to the states.⁷⁹ As noted in *Barker v. Wingo*,⁸⁰ the justifications for the right to a speedy trial include not

⁷² Fed. R. Evid. 807.

⁷³ *United States v. Dumeisi*, 424 F.3d 566 (7th Cir. 2005) (relying on trial court testimony that the foreign authorities had a duty to accurately record their own activities and the information received from their sources, a lack of motive to falsify information, and the fact that written records are often more reliable than the potentially hazy memory of the recorder).

⁷⁴ Fed. R. Evid. 801(d)(2).

⁷⁵ Mil. Comm. R. Evid. 802-803, available at [http://www.defense.gov/pubs/pdfs/Part%20III%20-%20MCREs%20\(FINAL\).pdf](http://www.defense.gov/pubs/pdfs/Part%20III%20-%20MCREs%20(FINAL).pdf) (last visited Mar. 13, 2010).

⁷⁶ *Id.*

⁷⁷ Mil. Comm. R. Evid. 803(c)

⁷⁸ U.S. CONST. amend. VI.

⁷⁹ *Klopfer v. North Carolina*, 386 U.S. 213, 226 (1967).

⁸⁰ 407 U.S. 514, 519 (1972).

only a concern regarding lengthy incarceration but also the interest of the American people in resolving criminal allegations in a timely and effective manner.⁸¹ Furthermore, the Supreme Court recognized “a societal interest in providing a speedy trial which exists separate from, and at times in opposition to, the rights of the accused.”⁸²

The right to speedy trial is codified for federal courts in the Federal Speedy Trial Act of 1974.⁸³ Under this Act, the Government is required to bring an indictment against a person within 30 days of his arrest, and the trial must commence within 70 days of indictment.⁸⁴ Nevertheless, the Supreme Court has qualified the right by stating that “not every constitutional provision applies to governmental activity even where the United States has sovereign power” and that “aliens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with the country.”⁸⁵ Moreover, the Federal Speedy Trial Act provides several specific exceptions to the timelines provided above. Relevant exceptions likely applicable to detainees include the “ends of justice” exception and the “unusual or complex” rationale for delaying trial.⁸⁶ Under either exception, a trial judge would be permitted to delay proceedings when he or she determines that a delay serves the “ends of justice” that outweigh the interests of the public and the accused in a speedy trial, or permit a delay when the facts at issue are “unusual or complex.”⁸⁷

Under the 2009 Amendments to the MCA, there are no statutory or procedural requirements addressing speedy trial in the case of enemy combatant detainees. Nevertheless, detainees tried by military commission will likely argue that the delay in prosecuting their cases violated their Fifth Amendment due process right by “caus[ing] substantial prejudice to [the detainees’] right to a fair trial.”⁸⁸

e. Right of Detainees to Confront Classified Information

One of the dilemmas facing prosecutors when trying persons associated with al Qaeda is the risk of disclosing classified information that could be useful to terrorist elements. Because of the Sixth Amendment requirement that “the

⁸¹ *Id.* at 519-20.

⁸² *Id.* at 519.

⁸³ 18 U.S.C. § 3161 (2006).

⁸⁴ *Id.* §§ 3161(b)-(c).

⁸⁵ *See Verdugo-Urquidez v. United States*, 494 U.S. 259, 268, 270-71 (1990) (internal citations omitted).

⁸⁶ 18 U.S.C. §§ 3161(h)(7)(A), 3161(h)(7)(B)(iii).

⁸⁷ *Id.* § 3161(h)(7)(B)(iii).

⁸⁸ *See United States v. Marion*, 404 U.S. 307, 324 (1971).

accused shall enjoy the right . . . to be confronted with the witnesses against him,”⁸⁹ the risk of disclosing classified information critical to successful prosecution presents a very real concern. This dilemma was a leading factor in the enactment of the Classified Information Procedures Act (“CIPA”), which aims to prevent the disclosure of classified information during criminal litigation while simultaneously providing the accused with sufficient information to craft a defense.⁹⁰ The Federal Rules of Criminal Procedure and CIPA both authorize federal judges to prevent the disclosure of classified information to the defendant in cases where nondisclosure would not prejudice his rights.⁹¹ Under these procedures, the judge may authorize the prosecution to provide substitute statements, or an unclassified summary, provided this alternative gives the defendant a real opportunity to challenge the prosecution’s evidence. In that regard, the redaction of any classified evidence may exclude sources and methods of intelligence gathering that do not go to the substance of what the evidence states, but rather simply do not identify the operatives or methods used. In all cases, however, the substitute must provide sufficient context such that the defendant has a real opportunity to discount or discredit the authenticity of the information being presented.

The protection of classified information and its disclosure in military commissions is addressed in the 2009 amendments to the Military Commissions Act.⁹² As amended, the MCA procedures are nearly identical to the practice under CIPA in federal courts. Under the 2009 procedures, the presiding military judge must allow the introduction of otherwise admissible evidence “while protecting from disclosure the sources, methods, or activities” through which the evidence was obtained.⁹³ The military judge may also order an *in camera* hearing to determine how the evidence shall be handled.⁹⁴ The accused may be excluded from such hearings as long as his attorney, who must have an appropriate security clearance, is permitted to argue for the release of the information on behalf of his client.⁹⁵ Under these procedures, the accused will have the opportunity to review all evidence actually submitted into the record and considered by the commission members.⁹⁶

⁸⁹ U.S. CONST. amend. VI.

⁹⁰ Pub. L. No. 96-456, 94 Stat. 2025, *codified at* 18 U.S.C. appx. 3 §§ 1-16 (2006).

⁹¹ *See* 18 U.S.C. appx. 3, § 3; Fed. R. Crim. P. 16(d)(1).

⁹² *See* 10 U.S.C. §§ 949p-1 *et seq.* (as added by Pub. L. No. 111-84 § 1802, 123 Stat. 2590 (2009)).

⁹³ *Id.* § 949p-6(c).

⁹⁴ *Id.* § 949p-6(c)(1).

⁹⁵ *Id.* § 949p-4.

⁹⁶ *Id.*

VI. OBSERVATIONS AND CONCLUSIONS

The upcoming prosecution of detainees in federal district court in New York and before military commissions, whether at Guantanamo or in the United States, will pose significant challenges to U.S. civilian and military prosecutors. U.S. Attorneys in New York, however, will likely face the greater difficulties. The federal court system and its Federal Rules of Criminal Procedure were not structured to try law-of-war violators who have been held without indictment and without access to the federal court system for a significant period of time.

Three specific areas will likely cause significant litigation on appeal should conviction lie in the district court. The first area of concern involves the right against self-incrimination under the Fifth Amendment and the likely debate in the courtroom concerning whether statements taken by U.S. officials using certain interrogation techniques were voluntary. In the military commission setting, the debate will center not on whether they are voluntary, but on the lesser standard of whether they are reliable and trustworthy.

A second major area of concern for the district court proceedings relates to the right of confrontation under the Sixth Amendment and the difficulty in ensuring the attendance of witnesses from abroad when not under the control of the U.S. government. In light of the more stringent rules regarding the admission of hearsay in federal court compared to the commission setting, procedural rules may limit the introduction of certain evidence in federal court unless it can be established as reliable under one of the exceptions to the hearsay rule.

The right to speedy trial may also prove troublesome for federal prosecutions. While there are exceptions provided, the right to speedy trial requires the Government to bring an indictment against a person within 30 days of his arrest, and the trial must commence within 70 days of indictment.⁹⁷ In no instance are these requirements met in any of the cases under consideration for prosecution. Even under the new amendments to the MCA, we can expect that detainees tried by military commission will raise the argument that their Fifth Amendment right to due process has been violated by the significant delay in prosecution.

These cases reflect the fact that careful consideration must be given when a Presidential Administration makes a choice of forum in national security cases. Any Obama Administration decision made without appreciating Congress' obvious recognition in the MCA of the need to tailor procedures to

⁹⁷ 18 U.S.C. §§ 3161(b), (c) (2006).

accommodate the nature of evidence available in these cases may cause prosecution hazards that could have been avoided.

RETIRING A “POLLUTING” FLEET: THE UNIQUE LEGAL CHALLENGES AND ENVIRONMENTAL HURDLES TO SUISUN BAY NON-RETENTION VESSEL DISPOSAL¹

Lieutenant Ryan M. Anderson²

I. INTRODUCTION

In 1949, following the end of World War II, the U.S. Secretary of Commerce was tasked with the disposal of all surplus merchant vessels exceeding a particular tonnage.³ In 1981, this disposal duty became a function of the U.S. Department of Transportation as a result of its acquisition of the U.S. Maritime Administration.⁴ The Maritime Administration currently maintains surplus vessels, which are referred to as the National Defense Reserve Fleet (“Reserve Fleet”).⁵ The Reserve Fleet is comprised primarily of three different fleets: The James River Reserve Fleet at Fort Eustis, Virginia; the Beaumont Reserve Fleet at Beaumont, Texas; and the Suisun Bay Reserve Fleet at Benicia, California.⁶

¹ Article current through March 1st, 2010.

² LL.M. Environmental and Natural Resources Law, Northwestern School of Law of Lewis & Clark College, 2009; J.D., The University of Montana School of Law, 2003; B.S. Forestry- Forest Resource Management (High Honors), The University of Montana, 1997. Presently assigned as Assistant Fleet Environmental Counsel to Commander, Fleet Forces Command in Norfolk, VA. This Article could not have been written without the thorough reviews by his LL.M. paper advisor, Professor William Funk. The Environmental faculty and LL.M. students at Lewis & Clark Law School helped the author focus on the most relevant issues. The author's positions and opinions do not represent the views of the U.S. Navy, the Department of Defense, or any other U.S. governmental agency.

³ Federal Property and Administrative Services Act of 1949 (as amended through Pub. L. 106-580 (2000)).

⁴ Maritime Act of 1981 § 2, Pub. L. No. 97-31, 95 Stat. 151, (1981) (as amended).

⁵ See, 50 U.S.C. §1744(1946) (The Merchant Sales Act of 1946, as amended):

The Secretary of Transportation shall maintain a National Defense Reserve Fleet, including any vessel assigned by the Secretary to the Ready Reserve Force component of the fleet, consisting of those vessels owned or acquired by the United States Government that the Secretary of Transportation, after consultation with the Secretary of the Navy, determines are of value for national defense purposes and that the Secretary of Transportation decides to place and maintain in the fleet.

⁶ Ship Disposal, http://www.marad.dot.gov/ships_shipping_landing_page/ship_disposal_program/Ship_Disposal_Program.htm (last visited Mar. 24, 2010).

The Reserve Fleet is currently comprised of four categories of vessels.⁷ One category consists of vessels owned by other government agencies that are simply maintained by the Maritime Administration.⁸ The other three categories of vessels are all owned by the Maritime Administration and are designated for different purposes. The three specific purposes include vessels dedicated to the Ready Reserve Fleet, vessels being preserved for federal agency programs, and vessels with insufficient value for commercial or military operation to warrant further preservation.⁹ Once a vessel is considered to be of insufficient value, it is categorized as a non-retention vessel.¹⁰

Until 1981, the primary method of disposal for non-retention vessels was through a competitive bidding process, which ultimately resulted in a sale.¹¹ The Maritime Administration's ship disposal program is now able to utilize appropriated funds to procure ship recycling and dismantling services.¹² The current program also allows the Maritime Administration to dispose of non-retention vessels through ship donation, artificial reefing, and SINKEXs (sink at-sea live-fire training exercises).¹³

On October 29, 2007, Arc Ecology, San Francisco Baykeeper, and Natural Resources Defense Council, Inc. (environmental plaintiffs) commenced suit against the Maritime Administration (to include Sean T. Connaughton in his capacity as Maritime Administrator, the U.S. Department of Transportation, and Mary E. Peters¹⁴ in her official capacity as Secretary of Transportation) in the U.S. District Court for the Eastern District of California.¹⁵ The suit alleged violations of the National Environmental Policy Act ("NEPA"), the Administrative Procedure Act ("APA"), the Resource Conservation and Recovery Act ("RCRA"), and the Federal Water Pollution Control Act ("CWA"). The allegations stemmed from the Maritime Administration's management and disposal of Reserve Fleet non-retention vessels located at Suisun Bay, CA.

This article provides background and summarizes the procedural history of the case against the Maritime Administration. The article then

⁷ Mar. Admin., U.S. Dep't of Transp., National Defense Reserve Fleet Inventory for the Month Ending January 31, 2009 (2009).

⁸ *Id.*

⁹ 46 U.S.C. § 57102(a) (2006).

¹⁰ *Id.*

¹¹ Ship Disposal, *supra* note 6.

¹² Floyd D. Spence National Defense Authorization Act of 2001 § 3502, Pub. L. No. 106-398 (2001).

¹³ Ship Disposal, *supra* note 6.

¹⁴ Mary E. Peters has been replaced by Ray H. LaHood.

¹⁵ Arc Ecology v. U.S. Mar. Admin., No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Oct. 29, 2007).

analyzes why the Maritime Administration was found to be in violation of the CWA and discusses the environmental obstacles to non-retention vessel disposal. The article then reviews Congress's failed attempts at disposing of the Suisun Bay non-retention fleet and recommends solutions to expedite non-retention vessel disposal. Lastly, the article discusses the limitations on available judicial remedies and the impact of this litigation on environmental progress.

II. BACKGROUND AND PROCEDURAL HISTORY

In order to dispose of a non-retention vessel at a location outside of northern California,¹⁶ the Maritime Administration is required to remove marine growth from the ship's hull.¹⁷ Until January of 2007, the marine growth was removed by "scamping." Scamping is a process in which the hulls of vessels are scraped, while remaining in the water, to remove soft aquatic species.¹⁸ On December 22, 2006, the California Regional Water Quality Control Board, San Francisco Bay Region ("California Water Quality Board"), advised the Maritime Administration that scamping results in discharges that threaten water quality standards.¹⁹ On January 22, 2007, the Maritime Administration issued a moratorium preventing further ship disposal from the Suisun Bay Reserve Fleet until a comprehensive agreement addressing vessel disposal impediments is entered into with state and federal officials.²⁰ On July 5, 2007, the Maritime Administration issued a letter announcing its intention to lift the moratorium and to resume disposing of vessels, notwithstanding the absence of a comprehensive agreement.²¹

On July 6, 2007, the California Water Quality Board informed the Maritime Administration that the unlawful discharges from its non-retention vessels violated the CWA and must be abated.²² It also ordered the Maritime Administration to prepare a mitigation plan which would address the removal of peeling paint from its non-retention vessels and ensure that no further discharges into Suisun Bay would occur.²³ Because the Maritime Administration refused to

¹⁶ See 33 C.F.R. §§ 3.55–1, 3.55–20 (1961) (as amended).

¹⁷ *Id.*

¹⁸ Mar. Admin., U.S. Dep't of Transp., Report to Congress on the Progress of the Vessel Disposal Program 3 (2008).

¹⁹ Complaint in Intervention at 11, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Nov. 14, 2008).

²⁰ Memorandum from the U.S. Dep't of Transp. Mar. Admin. Mar. Administrator to the Associate Administrator for National Security, et. al. (Jan. 22, 2007) (on file with author).

²¹ Memorandum from the U.S. Dep't of Transp. Mar. Admin. Mar. Administrator to Mr. Bruce H. Wolfe, Executive Officer, San Francisco Bay Regional Water Quality Control Board (Jul. 5, 2007) (on file with author).

²² Complaint in Intervention, *supra* note 19, at 10.

²³ *Id.*

submit a mitigation plan, the California Water Quality Board issued a notice of violation on October 1, 2007.

The Maritime Administration's announcement to lift the vessel disposal moratorium also led to the filing of *Arc Ecology v. U.S. Maritime Administration* on October 29, 2007. The plaintiffs alleged that the Maritime Administration had never performed an environmental analysis as mandated under NEPA on its plan to continue anchoring vessels in Suisun Bay, on its proposal for scamping vessels, nor on its planned disposal of vessels from the Suisun Bay Reserve Fleet.²⁴ As such, the plaintiffs alleged that the Maritime Administration had not evaluated the significant environmental effects of its disposal plan, had not considered less harmful alternatives, and had not solicited public involvement.²⁵

Relating to alleged violations of federal and state environmental laws, the plaintiffs claimed that scamping would release heavy metal-contaminated materials into the environment.²⁶ Furthermore, the plaintiffs alleged that the Maritime Administration's ship disposal plan would likely result in hazardous material leakage, invasive species conveyance, and aquatic species harm.²⁷ Specific to the CWA, the plaintiffs alleged that the Suisun Bay Reserve Fleet non-retention vessels are discharging and have discharged paint, corroded hull metal, polychlorinated biphenyls ("PCBs"), and other pollutants into Suisun Bay.²⁸

On March 28, 2008, the parties entered into a joint stipulation to stay all the NEPA and APA claims for relief.²⁹ The underlying basis for the stipulation was the Maritime Administration's preparation of an environmental assessment on the disposal of the Reserve Fleet vessels and its representation that a decision could be issued as early as late summer or fall 2008.³⁰ In the joint stipulation, the Maritime Administration agreed to not perform any scamping on non-retention vessels and to take no action to affect the movement of any non-retention vessels until it fully complied with the NEPA process.³¹ However, it reserved the right to move non-retention vessels in order to

²⁴ First Amended Complaint at 2, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Dec. 6, 2007).

²⁵ *Id.*

²⁶ *Id.* at 19.

²⁷ *Id.* at 23.

²⁸ *Id.* at 34.

²⁹ Joint Stipulation and Order Regarding Plaintiffs' NEPA Claims, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Mar. 28, 2008).

³⁰ Memorandum in Support of Defendants' Motion to Stay the Litigation of Plaintiffs' First, Second, Third, and Fourth Claims for Relief at 1, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Feb. 11, 2008).

³¹ Joint Stipulation and Order Regarding Plaintiffs' NEPA Claims, *supra* note 29, at 2.

experiment with respect to scamping, provided that approval is received from all the required federal and state agencies.³² The parties also agreed that the Maritime Administration could award contracts and move non-retention vessels to a dry-dock in the San Francisco Bay area for hull cleaning, remediation, and/or vessel recycling.³³

On November 14, 2008, the California Water Quality Board intervened in the suit. They claimed that because the non-retention vessels are highly deteriorated and in poor condition,³⁴ its applicable water quality objectives have been and continue to be violated by the Maritime Administration's refusal to remove its decaying ships from Suisun Bay.³⁵ The California Water Quality Board also alleged that the non-retention vessels are discharging heavy metals, paint chips, rust, corroded hull fragments, PCBs, asbestos, fuel, and oil into Suisun Bay in violation of § 301(a) of the CWA.

III. THE CWA CLAIM FOR RELIEF

The objective of the CWA is “to restore and maintain the chemical, physical, and biological integrity of the Nation’s waters.”³⁶ This objective is advanced by making the discharge of any pollutant by any person without a permit unlawful.³⁷ The term “discharge of a pollutant” and the term “discharge of pollutants” each mean any addition of any pollutant into navigable waters from any point source.³⁸

The environmental plaintiffs argued that Suisun Bay is a navigable water body and that the non-retention vessels, each individually (and/or, in the alternative, collectively), constitute a point source.³⁹ Further, the plaintiffs alleged that the Maritime Administration does not have, and never has had, a National Pollution Discharge Elimination System (“NPDES”) permit for discharge of any pollutant from any of the non-retention vessels.⁴⁰ As a consequence, plaintiffs alleged that the Maritime Administration has violated and is continuing to violate § 301(a) of the CWA.⁴¹

³² *Id.*

³³ *Id.*

³⁴ Complaint in Intervention, *supra* note 19, at 8.

³⁵ *Id.* at 9.

³⁶ Clean Water Act § 101(a), 33 U.S.C. § 1251(1948) (as amended).

³⁷ Clean Water Act § 301(a), 33 U.S.C. § 1311(a) (1948) (as amended).

³⁸ Clean Water Act § 502(12), 33 U.S.C. § 1362(12) (1948) (as amended).

³⁹ First Amended Complaint, *supra* note 24, at 34.

⁴⁰ *Id.*

⁴¹ *Id.*

The California Water Quality Board, the intervening plaintiff in the case, had a similar argument. In addition to the pollutants alleged by the environmental plaintiffs, it alleged that the non-retention vessels are also discharging heavy metals, rust, asbestos, fuel, oil, and contaminated hull biofouling organisms. They also alleged a broader geographical location (Suisun Bay and San Francisco Bay) and that the Maritime Administration's proposed in-water scamping of the non-retention vessels and its contemplated addition of more non-retention vessels to Suisun Bay each threaten to discharge additional pollutants.⁴²

At the time the lawsuit was filed, the Maritime Administration admitted that it did not have, and never has had, a NPDES permit for the discharge of any pollutant from any non-retention vessel.⁴³ In addition, the Maritime Administration did not challenge whether Suisun Bay is a navigable water of the U.S.⁴⁴ The term "navigable waters" means waters of the U.S. which are currently used, were used in the past, or may be susceptible to use in interstate or foreign commerce.⁴⁵ Suisun Bay is located approximately 23 nautical miles upstream from the main portion of San Francisco Bay.⁴⁶ The Suisun Bay Reserve Fleet anchorage has the capacity to moor several hundred ships and extends for approximately 4.5 nautical miles.⁴⁷

The term "vessel" is expressly included in the definition of point source.⁴⁸ Point source also includes the term "floating craft," which encompasses barges.⁴⁹ The CWA's definitions of both new and existing vessels "include every description of watercraft or other artificial contrivance used, or capable of being used, as a means of transportation on the navigable waters."⁵⁰ This definition is identical, in all relevant respects, to the definition contained in the General Provisions of the U.S. Code.⁵¹ In *U.S. v. Templeton*, the

⁴² Complaint in Intervention, *supra* note 19, at 12.

⁴³ Defendants' Answer to Plaintiffs' First Amended Complaint at 15, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Jan. 31, 2008).

⁴⁴ Memorandum of Points and Authorities in Support of Defendants' Motion for Partial Summary Judgment, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Sep. 9, 2009).

⁴⁵ 33 U.S.C. § 1362(7) (1948) (as amended); 40 C.F.R. § 122.2 (1983) (as amended).

⁴⁶ *Mar. Admin., U.S. Dep't of Transp., Removal of Non-Retention Vessels from National Defense Reserve Fleets for Disposal, Draft Programmatic Environmental Assessment 1-4* (Jun. 2008) [hereinafter "Maritime Administration's 2008 Environmental Assessment"].

⁴⁷ *Id.* at 1-5.

⁴⁸ 33 U.S.C. § 1362(14). The term "point source" means "any discernible, confined and discrete conveyance, including but not limited to any pipe, . . . conduit, . . . container, . . . or vessel or other floating craft, from which pollutants are or may be discharged."

⁴⁹ *United States v. West Indies Transp.*, 127 F.3d 299, 308 (3d Cir. 1997).

⁵⁰ *United States v. Templeton*, 378 F.3d 845, 849 (8th Cir. 2004) (citing § 312(a)(1)-(2); 33 U.S.C. § 1322(a)(1)-(2)).

⁵¹ *Templeton*, 378 F.3d at 849 (citing 1 U.S.C. § 3).

government argued that the *Rand*, a towboat restaurant, was not a vessel because its engines did not work, requiring it to be towed. The *Templeton* court held that inoperable engines and towing were not sufficient to disqualify the *Rand* as a vessel.⁵²

A more interesting issue was whether the non-retention vessels had added pollutants into Suisun Bay. The term “pollutant” means “dredged soil, solid waste, . . . chemical wastes, biological materials, . . . wrecked or discarded equipment . . . discharged into water.”⁵³ Although the Maritime Administration initially denied that its non-retention vessels are contaminated with toxic and hazardous wastes,⁵⁴ it did admit that certain non-retention vessels contain PCBs, mercury, oil, asbestos, and metals.⁵⁵ They also admitted that the exfoliation of paint on non-retention vessels has occurred and may continue to occur due to age and weathering.⁵⁶ Some of this exfoliated paint may disperse into the waters in which the vessels are anchored and the land under those waters.⁵⁷ In relation to the exterior surface of the non-retention vessels’ hulls, mercury and other metals are present in the paint.⁵⁸

On February 15, 2007, the Maritime Administration published a vessel environmental review report.⁵⁹ The vessel study, completed by a contracted third party, sampled and analyzed paint chips from forty Suisun Bay Reserve Fleet vessels, as well as collected and analyzed sediment found near the vessels.⁶⁰ The paint chips removed from the vessels indicated high concentrations of many toxic substances, to include zinc, copper, lead, hexavalent chromium, and mercury.⁶¹ An estimate of the total weight of seventeen different metals lost from the forty vessels exceeded 18,000 kilograms.⁶² The sediment sampled in the surrounding waters resulted in a finding that the same metals that were found in high concentrations in the paint chips were also present in high concentrations in the sediment.⁶³ In fact, two samples located 1,000 yards north and south of the non-retention vessels yielded

⁵² *Templeton*, 378 F.3d at 850.

⁵³ Clean Water Act § 502(6), 33 U.S.C. § 1362(6) (1948) (as amended).

⁵⁴ Defendants’ Answer to Plaintiffs’ First Amended Complaint, *supra* note 43, at 1.

⁵⁵ *Id.* at 2, 9-10.

⁵⁶ *Id.* at 8.

⁵⁷ *Id.* at 9-10.

⁵⁸ *Id.*

⁵⁹ Mar. Admin., U.S. Dep’t of Transp., National Defense Reserve Fleet (NDRF), Suisun Bay, CA, Vessel Environmental Review (Feb. 15, 2007).

⁶⁰ *Id.* at ES-1.

⁶¹ *Id.* at ES-2.

⁶² *Id.* at ES-3.

⁶³ *Id.* at ES-4.

the same results as the sediment samples removed from the immediate anchorage area.⁶⁴

The environmental review report also cast some doubt on the Maritime Administration's responsibility for Suisun Bay's contamination. For example, the estimate of lost paint is qualified by a statement that "not all the missing paints have necessarily been lost at the present locations of the vessels in Suisun Bay."⁶⁵ The report concluded with a finding indicating that the 18,000 kilograms of lost paint from the forty sampled vessels cannot be interpreted to be the only source or even a partial contributor to the observed sediment contamination because of a variety of other possible sources in the area.⁶⁶ The other sources in the area include industrial and municipal wastewater dischargers, non-point source surface runoff, and atmospheric deposition.⁶⁷ Interestingly, the report concluded with a statement that the data cannot be interpreted to imply that releases of toxic metals from the non-retention vessels "have not occurred in the past and/or are not currently taking place."⁶⁸

In September 2009, the Maritime Administration finally represented that it was not disputing that the release of exfoliating paint and debris from its non-retention vessels constitutes the "discharge of a pollutant."⁶⁹ While no quantifiable requirement exists to prove an addition, an independent third party contracted by the Maritime Administration estimated a loss of approximately 18,000 kilograms of paint from forty of the non-retention vessels in Suisun Bay. The sediment sampling revealed actual pieces of corroded metal with barnacle growth, which presumably ablated off a nearby vessel.⁷⁰ In addition, paint chips fall within the CWA's broad definition of pollutant.⁷¹ Furthermore, the sediment analysis revealed high concentrations of a number of heavy metals, the same metals that were found in high concentrations in the paint chips. As such, the Maritime Administration would most likely have lost credibility by challenging this issue.

Although the Maritime Administration decided not to dispute that its non-retention vessels were discharging pollutants, the agency continued to

⁶⁴ Mar. Admin., U.S. Dep't of Transp., National Defense Reserve Fleet (NDRF), Suisun Bay, CA, Vessel Environmental Review (Feb. 15, 2007), at ES-4.

⁶⁵ *Id.* at ES-3.

⁶⁶ *Id.* at ES-5.

⁶⁷ *Id.* at ES-6.

⁶⁸ *Id.*

⁶⁹ Memorandum of Points and Authorities in Support of Defendants' Motion for Partial Summary Judgment, *supra* note 44, at 22.

⁷⁰ Mar. Admin., U.S. Dep't of Transp., National Defense Reserve Fleet (NDRF), Suisun Bay, CA, Vessel Environmental Review 35 (Feb. 15, 2007).

⁷¹ *West Indies Transp.*, 127 F.3d at 308.

challenge the CWA claims. On September 8, 2009, the Maritime Administration attempted to moot the Plaintiffs' CWA claims by filing a "Notice of Intent" to comply with the terms of the California Water Quality Board's Storm Water General Permit.⁷² Dischargers of storm water associated with industrial activity are required to either apply for an individual permit or seek coverage under the promulgated storm water general permit.⁷³ To receive authorization to discharge under the general permit, each eligible discharger must submit a Notice of Intent to be authorized.⁷⁴ The Maritime Administration also prepared the requisite Storm Water Pollution Prevention Plan which encompassed both its non-retention vessels and all its waterfront industrial activities.⁷⁵ Under the general permit, industrial activities specified in the Notice of Intent are authorized unless and until the Regional Water Board or the California Water Quality Board take some action to deny coverage.⁷⁶

On September 10, 2009, the California Water Quality Board indicated to the Maritime Administration that the Suisun Bay Reserve Fleet facility is not eligible for coverage under the general permit and that its notice to seek coverage under that permit will be terminated.⁷⁷ The California Water Quality Board opined that even if the storm water general permit applied to the non-retention vessel site, the permit does not authorize non-storm water discharges.⁷⁸ The California Water Quality Board further clarified its position by stating that the general permit covers storm water discharges, meaning discharges from rain, and that the non-retention vessels discharge paint into Suisun Bay even when it is not raining, such as when peeling paint falls off the vessels' exterior hulls and when paint blows off vessels' decks in the wind.⁷⁹

On November 9, 2009, during the partial summary judgment proceeding's oral argument, the Maritime Administration indicated that it is in

⁷² Memorandum of Points and Authorities in Support of Defendants' Motion for Partial Summary Judgment, *supra* note 44, at 22. The Maritime Administration qualified its position that the General Permit is the proper NPDES permit for the industrial activities and associated discharges at the Suisun Bay Reserve Fleet by stating that its position is based solely on the applicable California laws and regulations and the unique nature of the Suisun Bay Reserve Fleet and the non-retention vessels at issue in this litigation.

⁷³ *Id.* at 13 (citing 40 C.F.R. §§122.26(a)(1)(ii) and 122.26(c)).

⁷⁴ *Id.* at 12 (citing 40 C.F.R. §122.28(b)(2)(i)).

⁷⁵ *Id.* at 22.

⁷⁶ *Id.* at 23.

⁷⁷ Plaintiffs and Plaintiff-Intervenor's Joint Statement of Undisputed Facts in Support of Motions for Partial Summary Judgment of Liability at 35, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Sep.15, 2009).

⁷⁸ Plaintiffs' Opening Brief in Support of Motion for Partial Summary Judgment of Liability on Claims 5, 6, and 7 at 34, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Sep.14, 2009).

⁷⁹ Plaintiffs' Brief in Opposition to Defendants' Motion for Partial Summary Judgment at 4, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Sep.29, 2009).

violation of the CWA.⁸⁰ On January 20, 2010, the court ruled on the partial summary judgment motion as follows: that the non-retention vessels are point sources subject to the permitting requirements of the CWA;⁸¹ that Suisun Bay is navigable water within the meaning of the CWA;⁸² and that exfoliated paint and other materials discharged from the non-retention vessels to Suisun Bay are pollutants under the CWA.⁸³ The court therefore held that since at least October 5, 2007, the Maritime Administration has been and continues to be in violation of § 301(a) of the CWA by discharging pollutants from each non-retention vessel into the waters of Suisun Bay without a valid NPDES permit.⁸⁴

IV. ENVIRONMENTAL OBSTACLES TO NON-RETENTION VESSEL DISPOSAL

As analyzed *supra*, the environmental and intervening plaintiffs have valid concerns regarding the Maritime Administration's violations of state and federal environmental laws. All that remains to litigate in the case is the Maritime Administration's scope of liability for the clean-up and remediation of the Suisun Bay Reserve Fleet site and the scope of the injunction the court will likely issue to prevent future environmental violations.⁸⁵ The court will likely require extensive briefing from the parties in order to fashion an adequate remedy. The collection of impediments to the Maritime Administration's lawful disposal of non-retention vessels is a legal quagmire. The simple remedies of preventing pollution by turning off a valve or ordering the defendants to cease production simply are not available. The following sections analyze the major legal impediments.

A. National Invasive Species Act ("NISA")⁸⁶

The Maritime Administration's most frequently utilized method of non-retention vessel disposal is ship recycling.⁸⁷ In the Suisun Bay area, there exists one provisionally approved ship recycling facility. The facility is located on Mare Island, California, approximately 42 miles from the non-retention

⁸⁰ Reporter's Transcript, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Nov. 9, 2009).

⁸¹ Order on Cross Motions for Partial Summary Judgment at 3, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Jan. 20, 2010) (citing 33 U.S.C. §§ 1362(14), 1311(a)).

⁸² *Id.* at 4 (citing 33 U.S.C. § 1362(7)).

⁸³ *Id.* at 4 (citing 33 U.S.C. § 1362(6)).

⁸⁴ *Id.* at 4.

⁸⁵ The trial is currently scheduled for June 2010. See Marcus Wohlsen, *Judge: Calif. Ghost Fleet Breaks Pollution Laws*, ASSOCIATED PRESS, Jan. 22, 2010.

⁸⁶ National Invasive Species Act of 1996, Pub. L. 104-332 (1996) (as amended). "To provide for ballast water management to prevent the introduction and spread of nonindigenous species into the waters of the United States, and for other purposes."

⁸⁷ Maritime Administration's 2008 Environmental Assessment, *supra* note 46, at 2-13.

vessels.⁸⁸ Provisional approval means the facility is not operational and has yet to acquire the necessary permits.⁸⁹ The inability to acquire the necessary permits allegedly stems from the facility's inability to obtain a dredging permit to deepen the Mare Island Strait, which is required to enable the passage of the non-retention vessels from Suisun Bay.⁹⁰ According to the facility, the California Department of Toxic Substances Control believes the strait may be contaminated and wants the proposed facility to fund a \$1.2 million sampling study of the materials to be dredged.⁹¹ Six other fully approved ship recycling facilities exist in the U.S., none of which are on the west coast.⁹²

Because the majority of vessels managed by the Maritime Administration have remained at anchorage for a number of years, underwater marine growth has accumulated.⁹³ In 2006, the Maritime Administration was notified by the U.S. Coast Guard that its non-retention vessels were required to comply with the Coast Guard's National Invasive Species Act implementing regulations.⁹⁴ As a means of reducing the spread of invasive species, the Coast Guard requires that marine growth be removed from all non-retention vessels that are scheduled to be removed from one bio-geographical area into another bio-geographical area for final disposal.⁹⁵ Non-retention vessels remaining in the same bio-geographical region as its fleet anchorage do not require hull marine growth removal.⁹⁶ Bio-geographic regions have been interpreted to be those areas typically restricted to the cognizance of the same Coast Guard Captain of the Port.⁹⁷ The requirement for marine growth removal when a vessel travels outside its bio-geographical area, coupled with the reality that an approved recycling facility does not exist in the Suisun Bay area, mandates that every non-retention vessel to be disposed of requires marine growth removal.

B. In-Water Marine Growth Removal Issues

In December 2006, the California Department of Toxic Substances performed an analytical test of the organisms and paint removed from two non-retention vessels.⁹⁸ According to them, the test confirmed that scamping would

⁸⁸ *Id.* at 2-21.

⁸⁹ *Id.*

⁹⁰ Jessica A. York, *Mare Island Dredging is Final Hurdle Delaying Use of Dry Docks*, THE VALLEJO TIME HERALD, Feb. 4, 2009.

⁹¹ *Id.*

⁹² Maritime Administration's 2008 Environmental Assessment, *supra* note 46, at 2-13.

⁹³ *Id.* at 2-11.

⁹⁴ *Id.* "As implemented by 33 C.F.R. Part 151, Subpart D (pertaining to aquatic hull growth) (effective in September 2004)."

⁹⁵ *Id.*

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ Complaint in Intervention, *supra* note 19, at 11.

discharge unacceptable levels of copper, chromium, and zinc into San Francisco Bay.⁹⁹ In early 2007 the Maritime Administration tested its proposed scamping method on a Reserve Fleet vessel located in the James River Reserve Fleet at Fort Eustis, Virginia. The California Water Quality Board reviewed the results of that test and determined that the dissolved copper and zinc concentrations in the vicinity of the active scamping device significantly exceeded background concentrations in an amount that would violate California Water Quality Standards.¹⁰⁰

As a result of its determination, the California Water Quality Board claims that the scamping device used in the James River test “may be precluded in California waters absent a specific NPDES permit.”¹⁰¹ Furthermore, the California Water Quality Board states that the issuance of a NPDES permit would require significant study and regulatory review, which may result in not allowing the discharge without significant modification of the scamping device.¹⁰² Pursuant to California law,¹⁰³ the California Water Quality Board ordered the Maritime Administration to provide a “Scamping Pilot Test Workplan” that specifies “sampling and analysis methods and protective measures for a proposed scamping technology pilot test in State of California waters” at least 45 days prior to any proposed pilot test.¹⁰⁴ The Maritime Administration has not complied with this order to provide a work plan.¹⁰⁵

The Maritime Administration avers that “it would endeavor to capture in nylon bags some of the material that is removed during a contained scamping process” and “that any captured materials would be removed for disposal.”¹⁰⁶ Further, it does not contest that scamping can cause the removal of some soft and hard marine growth or paint or hull fragments from some vessels.¹⁰⁷ The Maritime Administration disclosed that scamping can result in discharges of some pollutants from some vessels but that this occurrence depends upon the

⁹⁹ *Id.*

¹⁰⁰ *Id.* at 11-12.

¹⁰¹ Memorandum from the California Regional Water Quality Control Board, San Francisco Bay Region, Senior Staff Counsel to the U.S. Dep’t of Transp. Sec. of Transp. et. al. (Aug. 27, 2008) (on file with author).

¹⁰² *Id.*

¹⁰³ See California Water Code § 13267(b)(1) “. . . the regional board may require that any person who . . . proposes to discharge waste within its region . . . shall furnish . . . technical or monitoring program reports which the regional board requires.”

¹⁰⁴ Memorandum from the California Regional Water Quality Control Board, San Francisco Bay Region, Senior Staff Counsel to the U.S. Dep’t of Transp. Sec. of Transp. et. al., 7 (Aug. 27, 2008) (on file with author).

¹⁰⁵ Complaint in Intervention, *supra* note 19, at 12.

¹⁰⁶ Defendants’ Answer to Plaintiffs’ First Amended Complaint, *supra* note 43, at 7.

¹⁰⁷ Defendants’ Answer to Plaintiff-Intervenor’s Complaint in Intervention at 8-9, Arc Ecology v. U.S. Mar. Admin., No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Jan. 12, 2009).

specific use of the scamping apparatus.¹⁰⁸ In addition, they are not aware of any other commercially available in-water hull cleaning process that captures any of the discharge from the scamping machine.¹⁰⁹ As such, the Maritime Administration still believes that the proposed scamping method which was tested in 2007 and summarily rejected by the California Water Quality Board is the best method available.

Although the Coast Guard sanctioned the Maritime Administration's in-water hull cleaning method to remove hull marine growth,¹¹⁰ the California Water Quality Board has yet to change its position. As a result, the implication is that the only lawful means of removing hull marine growth available to the Maritime Administration is the utilization of a dry-dock.

On August 31, 2009, the Maritime Administration released its final programmatic environmental assessment for the removal and disposal of non-retention vessels from the National Defense Reserve Fleet.¹¹¹ In the environmental assessment, the Maritime Administration represented for the first time during the pendency of the case that dry-docking, if practicable, will be the preferred method of underwater hull cleaning for non-retention vessels.¹¹² The Maritime Administration qualified its new policy by stating that dry-docking is limited by several factors, to include: The risk and liability issues associated with dry-docking older ships that are in poor material condition; the existence of just two operating dry-docks in the San Francisco Bay area; and the availability and cost of those dry-docks to accomplish hull cleaning.¹¹³ The Maritime Administration's earlier position during the case was that dry-docking had not been utilized for marine growth removal for any non-retention vessels because of competition with the private sector, the structural integrity on the non-retention vessels and the estimated cost of dry-docking.¹¹⁴

Although the Maritime Administration now represents that dry-docking is its preferred method for marine growth removal, it also represents that in-water hull cleaning may still be utilized on a case-by-case basis if a non-retention vessel's hull is determined to be too fragile or too high-risk for dry

¹⁰⁸ *Id.*

¹⁰⁹ Memorandum of Points and Authorities in Support of Defendants' Motion for Partial Summary Judgment, *supra* note 44, at 9.

¹¹⁰ Mar. Admin., U.S. Dep't of Transp., Report to Congress on the Progress of the Vessel Disposal Program 3 (Jan. 2008).

¹¹¹ Mar. Admin., U.S. Dep't of Transp., Removal and Disposal of Non-Retention Vessels from National Defense Reserve Fleet, Final Programmatic Environmental Assessment (Aug. 2009) [hereinafter "Maritime Administration's 2009 Final Environmental Assessment"].

¹¹² *Id.* at 41.

¹¹³ *Id.* at 42.

¹¹⁴ Maritime Administration's 2008 Environmental Assessment, *supra* note 46, at 2-13.

docking.¹¹⁵ The Maritime Administration also qualified its new in-water hull cleaning policy by stating that the in-water cleaning of non-retention vessels will not occur unless permitted by the California Water Quality Board.¹¹⁶

Because the California Water Quality Board will not allow the Maritime Administration to scamp its vessels in Suisun Bay and because the feasibility of dry-docking is a function of funding, vessel material readiness and dry-dock availability, the non-retention vessels in Suisun Bay will remain at anchorage for the foreseeable future. If the Maritime Administration were able to use its scamping method on the non-retention vessels for marine growth removal, the vessels could be more quickly removed from Suisun Bay and transferred to recycling facilities in the Atlantic and Gulf of Mexico regions.

C. Anti-Degradation

The California State Water Resources Control Board (“California Water Resources Board”) administers the CWA on behalf of the U.S. Environmental Protection Agency (“EPA”).¹¹⁷ In order to carry out the CWA’s objectives, the California Water Resources Board is required to identify technology-based effluent limitations for point sources¹¹⁸ and secondary treatment effluent limitations for publicly owned treatment works.¹¹⁹ In addition, it is required to identify and implement water quality standards.¹²⁰ Water quality standards are identified by reviewing the designated uses of the navigable water involved and the water quality criteria required to maintain such use.¹²¹ Once a designated use is identified, the California Water Resources Board can remove the use only if a determination is made that the designated use was never achievable. Once effluent limitations and water quality standards are determined, they are required to survey its navigable water segments. During the survey, they must identify the water segments in which the effluent limitations determined are not stringent enough to maintain the applicable water quality standard(s).¹²² Once a water segment is identified, the California Water Resources Board is required to determine the total maximum daily load of pollutants allowed for the water segment.¹²³

¹¹⁵ Maritime Administration’s 2009 Environmental Assessment, *supra* note 111, at 39, 169.

¹¹⁶ *Id.* at 175.

¹¹⁷ See 33 U.S.C. §§ 1314(i), 1342(b) (1948) (as amended); 40 C.F.R. § 123.25 (1983) (as amended).

¹¹⁸ Clean Water Act §301(b)(1)(A), 33 U.S.C. § 1311(b)(1)(A) (1948) (as amended).

¹¹⁹ Clean Water Act §301(b)(1)(B), 33 U.S.C. § 1311(b)(1)(B) (1948) (as amended).

¹²⁰ Clean Water Act §303, 33 U.S.C. § 1313 (1948) (as amended).

¹²¹ Clean Water Act §303(c), 33 U.S.C. § 1313(c) (1948) (as amended).

¹²² Clean Water Act §303(d)(1)(A), 33 U.S.C. § 1313(d)(1)(A) (1948) (as amended).

¹²³ Clean Water Act §303(d)(1)(C), 33 U.S.C. § 1313(d)(1)(C) (1948) (as amended).

Suisun Bay's effluent limitations are not stringent enough to maintain its water quality standards. As such, Suisun Bay is impaired and is water quality limited for several pollutants, to include, *inter alia*, mercury, nickel, and PCBs.¹²⁴ In its prayer for relief, the CA Water Quality Board requested the court to order the Maritime Administration to comply with the CWA by either ceasing discharges from the non-retention vessels or by obtaining a valid NPDES permit.¹²⁵ Because the Maritime Administration is constrained in its ability to move the non-retention vessels, they will have a difficult time ceasing the discharges. If the Maritime Administration applied for the requisite NPDES permit, it is unlikely that the CA Water Quality Board would issue it since the EPA has promulgated regulations precluding the issuance of any permit "when the imposition of conditions cannot ensure compliance with the applicable water quality requirements of all affected States"¹²⁶ and when the issuance of a permit to a new source or discharger will cause or contribute to a water quality standard violation.¹²⁷ Therefore, the Maritime Administration would only be issued a permit if it could demonstrate that "there are sufficient remaining pollutant load allocations to allow for the discharge" and that "the existing dischargers into that segment [Suisun Bay] are subject to compliance schedules designed to bring the segment into compliance with applicable water quality standards."¹²⁸

Because Suisun Bay is water-quality limited for a number of the same pollutants that the Maritime Administration would need to apply for in a permit application, it would have difficulty meeting its burden to show that "there are sufficient remaining pollutant load allocations." As such, the likelihood that the California Water Quality Board would approve the permit is remote. Because the California Water Quality Board asserts that the non-retention vessels are causing or contributing to Suisun Bay's further impairment and is lowering its water quality in violation of the CWA's anti-degradation requirements,¹²⁹ California would have a difficult time defending its issuance of a NPDES permit for discharges from the non-retention vessels. The Maritime Administration is also not able to be issued a discharge permit even if it agrees to remediate the same water quality limited segment for the same pollutant for which it desires to discharge. The Ninth Circuit Court of Appeals has held that such a method of

¹²⁴ Complaint in Intervention, *supra* note 19, at 2; San Francisco Bay Regional Board, Proposed 2006 CWA Section 303(d) List of Water Quality Limited Segments 31-32.

¹²⁵ Complaint in Intervention, *supra* note 19, at 13.

¹²⁶ 40 C.F.R. § 122.4(d) (1983) (as amended).

¹²⁷ 40 C.F.R. § 122.4(i) (1983) (as amended).

¹²⁸ *Id.*

¹²⁹ Complaint in Intervention, *supra* note 19, at 10; *see* Clean Water Act § 303(d)(4)(B), 33 U.S.C. § 1313 (1948) (as amended).

offsetting is not allowed under the plain language of the regulations implementing the CWA.¹³⁰

D. Legal Impediments to Foreign Ship Recycling

Between 1983 and 1994, approximately 173 Reserve Fleet non-retention vessels were towed overseas for foreign ship recycling.¹³¹ In October of 2000, foreign vessel recycling was reinvigorated when Congress directed that the Maritime Administration may scrap obsolete vessels in accordance with law¹³² through the use of qualified scrapping facilities, using the most expeditious scrapping methodology and location as practicable.¹³³ Congress specifically directed that the scrapping facilities shall be selected

on a best value basis without any predisposition toward foreign or domestic facilities taking into consideration, among other things, the ability of facilities to scrap vessels: (1) at least cost to the Government; (2) in a timely manner; (3) giving consideration to worker safety and the environment; and (4) in a manner that minimizes the geographic distance that a vessel must be towed when towing a vessel poses a serious threat to the environment.¹³⁴

A “large demand for scrap metal on the international markets” continues to exist and the Maritime Administration continues to be approached by foreign ship recyclers to purchase its non-retention vessels.¹³⁵ However, a number of international environmental laws, as well as federal environmental laws, currently restrict the export of non-retention vessels.¹³⁶ In its 2008 Draft Programmatic Environmental Assessment, the Maritime Administration dismissed an alternative to sell vessels to foreign recyclers, asserting that “due to

¹³⁰ *Friends of Pinto Creek v. United States EPA*, 504 F.3d 1007 (9th Cir. 2007).

¹³¹ Maritime Administration’s 2008 Environmental Assessment, *supra* note 46, at 4-13; *see also*, Bob Stump National Defense Authorization Act for Fiscal Year 2003, Pub. L. No. 107-314, § 3504(c), 116 Stat. 2458, 2755-56 (2002). Four vessels were also towed from the James River Reserve Fleet to the United Kingdom in 2003 as part of a pilot program to study whether international ship-breaking could be done in an environmentally friendly manner.

¹³² National Maritime Heritage Act of 1994, Pub. L. No. 103-451, 108 Stat. 4769, 4777 (codified as amended at 16 U.S.C. § 5405 (2008)).

¹³³ Floyd D. Spence National Defense Authorization Act of 2001, Pub. L. No. 106-398, § 3502(b) (2000).

¹³⁴ *Id.*

¹³⁵ Maritime Administration’s 2008 Environmental Assessment, *supra* note 46, at 2-34.

¹³⁶ For an in-depth analysis of international and U.S. domestic laws governing the export of hazardous materials, *see* Takako Morita, *N.I.M.B.Y. Syndrome and the Ticking Time Bomb: Disputes Over the Dismantling of Naval Obsolete Vessels*, 17 GEO. INT’L ENVTL. L. REV. 723, 726 (2005).

the environmental impediments of the Toxic Substances Control Act (TSCA),¹³⁷ which delays the export of non-retention vessels containing PCBs, foreign sales currently are not legally practicable.”¹³⁸

On August 18, 2008, legislation was enacted which further frustrated the export of non-retention vessels for the purpose of dismantling, recycling, or scrapping.¹³⁹ Generally, the legislation now prevents the exporting of vessels to foreign countries for disposal unless the Maritime Administration can certify to two committees of Congress that a compelling need for the vessel’s dismantling, recycling, or scrapping exists and that there is no available capacity to dispose of the vessel in the U.S.¹⁴⁰ In addition, the Maritime Administration would need to show that the foreign country’s vessel disposal methods would be conducted in full compliance with equivalent U.S. environmental, safety, labor, and health requirements.¹⁴¹ Because stateside non-retention vessel recycling capacity exists, the Maritime Administration would have difficulty convincing Congress to allow it to enter into foreign disposal contracts.

V. CONGRESSIONAL ATTEMPTS TO DISPOSE OF NON-RETENTION VESSELS

Congress originally directed the Maritime Administration to dispose of all Reserve Fleet non-retention vessels by September 30, 1999.¹⁴² However, this deadline was extended to September 30, 2001.¹⁴³ In October of 2000, Congress again extended the disposal deadline to September 30, 2006.¹⁴⁴ When extending the deadline for the second time, Congress specifically directed that the Secretary of Transportation “shall prepare, publish and submit to Congress . . . a

¹³⁷ See 15 U.S.C. § 2605(e)(2)(A) (1976) (as amended). “No person may manufacture, process, or distribute in commerce or use any polychlorinated biphenyl in any manner other than in a totally enclosed manner.” See also 15 U.S.C. § 2605(e)(2)(B) (1976) (as amended):

The Administrator may by rule authorize the manufacture, processing, distribution in commerce or use (or any combination of such activities) of any polychlorinated biphenyl in a manner other than in a totally enclosed manner if the Administrator finds that such manufacture, processing, distribution in commerce, or use (or combination of such activities) will not present an unreasonable risk of injury to health or the environment.

¹³⁸ Maritime Administration’s 2008 Environmental Assessment, *supra* note 46, at 2-35.

¹³⁹ Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 § 3502, Pub. L. No. 110-417, 122 Stat. 4761 (2008).

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² See National Maritime Heritage Act of 1994, Pub. L. No. 103-451, 108 Stat. 4769, 4777 (codified as amended at 16 U.S.C. § 5405 (2008)).

¹⁴³ National Defense Authorization Act for Fiscal Year 1998, Pub. L. No. 105-85, 111 Stat. 1878, § 102(c)(1)(A) (1997).

¹⁴⁴ Floyd D. Spence National Defense Authorization Act of 2001, Pub. L. No. 106-398, § 3502 (2000).

comprehensive plan for management of the vessel disposal program of the Maritime Administration . . .”¹⁴⁵ The management plan called for a strategy to dispose of the Reserve Fleet non-retention vessels maximizing the “use of all available disposal methods, including dismantling, use for artificial reefs, donation, and Navy training exercises.”¹⁴⁶ In carrying out the directive, the Secretary of Transportation was directed to dispose of all vessels in a timely, safe and environmentally sound manner.¹⁴⁷ The Maritime Administration complied with Congress’s directive to prepare a comprehensive management plan,¹⁴⁸ but has obviously failed to dispose of all the non-retention vessels within the specified timeframe.

The Maritime Administration’s 2006 comprehensive management plan projected an average disposal cost of \$2.5 million per non-retention vessel and contemplated expediting the disposal of high priority vessels.¹⁴⁹ The plan also considered the removal of twenty to twenty-four vessels a year and intended to only maintain low priority/low risk vessels at the fleet sites.¹⁵⁰ However, the plan qualified its success on the viability of foreign recycling and funding that allows for economies of scale.¹⁵¹

Because of the large number of non-retention vessels in queue for disposal and the cost associated with each vessel, the Maritime Administration ultimately determined that Congress’s 2006 disposal mandate was not realistic.¹⁵² It further posited that additional time was required

to dispose of all non-retention vessels due to limited capacity available for recycling vessels, the continuing addition of non-retention vessels to the [Reserve Fleet], the need to ensure compliance with all applicable federal and state laws and regulations relating to the various vessel disposal options, and the need to fully address concerns from the public.”¹⁵³

As an example, the Maritime Administration asserts that from 2001-2005 it received 73 additional non-retention vessels. It maintains that because it is the

¹⁴⁵ *Id.*

¹⁴⁶ *Id.*

¹⁴⁷ Maritime Administration’s 2008 Environmental Assessment, *supra* note 46, at 1-7.

¹⁴⁸ See Mar. Admin., U.S. Dep’t of Transp., Comprehensive Management Plan for the Disposal of Maritime Administration (MARAD) Non-Retention Vessels FY 2006 (2006).

¹⁴⁹ *Id.* at 1, 6. “Vessels with hull conditions of #0, 1 and 2 are considered to be high priority for disposal and are considered to be a high environmental risk due to the potential for oil discharges through breaches in the hull.”

¹⁵⁰ *Id.* at 6.

¹⁵¹ *Id.* at 7.

¹⁵² *Id.*

¹⁵³ Maritime Administration’s 2008 Environmental Assessment, *supra* note 46, at 1-3.

disposal agent for all federally owned merchant vessels, it “is subject to receiving obsolete ships into its disposal regime on a continuing basis for the foreseeable future.”¹⁵⁴

VI. PROPOSED SOLUTIONS FOR CWA COMPLIANCE AND REMOVAL OF NON-RETENTION VESSELS FROM SUISUN BAY

The Maritime Administration should pursue a two-tiered process to expedite the removal of its non-retention vessels from Suisun Bay. The first tier in the process requires the Maritime Administration to reconsider its practical alternatives. It should conduct a study of its Suisun Bay vessel disposal program to determine exactly what effluent limitations would be required in order to comply with the CWA and then apply for a NPDES permit. If the permit application is ultimately denied by the California Water Quality Board, at least the Maritime Administration would have exhausted that possible solution. In addition, the Maritime Administration should commit more resources to locating and engaging the private industry in the dry-dock and ship recycling business.

If the Maritime Administration is still unable to dispose of its non-retention vessels after exhausting all of its practical alternatives, it should move to the second tier of the process. The second tier includes three possible legal solutions to non-retention vessel disposal. The first possible legal solution relates to the interpretation of the Coast Guard regulations requiring marine growth removal. As detailed *supra*, the Maritime Administration’s ability to dispose of its non-retention vessels in another bio-geographical area of the U.S. is frustrated by the Coast Guard regulation relating to hull marine growth. Specifically, the regulation requiring ballast water management practices mandates the removal of fouling organisms from hull, piping, and tanks on a regular basis and the disposal of any removed substances in accordance with local, state and federal regulations.¹⁵⁵ The Coast Guard has determined that its regulations apply to the aquatic growth on the hulls of non-retention vessels under tow.¹⁵⁶

With that said, the regulations only apply to vessels that “operate” in the waters of the U.S. and are bound for ports or places in the U.S.¹⁵⁷ The Maritime Administration could attempt to convince the Coast Guard to change its position because its non-retention vessels are removed from Suisun Bay

¹⁵⁴ Mar. Admin., U.S. Dep’t of Transp., Comprehensive Management Plan for the Disposal of Maritime Administration (MARAD) Non-Retention Vessels FY 2006 1 (2006).

¹⁵⁵ 33 C.F.R. § 151.2035 (1999) (as amended).

¹⁵⁶ Memorandum of Points and Authorities in Support of Defendants’ Motion for Partial Summary Judgment, *supra* note 44, at 7.

¹⁵⁷ 33 C.F.R. § 151.2005 (1999) (as amended).

under tow from another vessel and because the non-retention vessels do not operate in the waters of the U.S. as contemplated by the regulation. The word “operate” has not been defined by statute, regulation, or case law in relation to the hull marine growth regulation. Such an interpretation is legally defensible and would allow the Maritime Administration to remove its non-retention vessels from Suisun Bay without any amendment to current law.

If the Maritime Administration’s attempt to convince the Coast Guard that its non-retention vessels do not operate as contemplated in the marine growth regulation is unsuccessful, it may nonetheless be able to dispose of the vessels by utilizing the second proposed legal solution, the U.S. Navy’s SINKEX program. The EPA has issued the Navy a general permit to transport vessels from the U.S. for the purpose of sinking such vessels in ocean waters for testing ordnance.¹⁵⁸ The general permit requires that all vessel sinkings be conducted in water at least 6,000 feet deep and at least fifty nautical miles from land.¹⁵⁹ Because the marine growth removal regulation only applies if the non-retention vessels are bound for ports or places in another bio-geographical area of the U.S.¹⁶⁰ and because the vessels designated for SINKEX would be bound for the open ocean, the regulation would not apply.

However, the general permit does require that appropriate measures be taken prior to vessel sinking to remove to the maximum extent practicable all materials which may degrade the marine environment.¹⁶¹ Such measures include removing from the hulls other pollutants and all readily detachable material capable of creating debris or contributing to chemical pollution.¹⁶² To not run afoul of its general permit requirements, the Navy would have to posit that marine growth removal is not practicable or that marine growth is not a pollutant or readily detachable material capable of creating debris. The Navy would also need to determine that the removal of underwater paint is either not practicable or that the paint would not contribute to chemical pollution. The reasonableness of such a position would depend on the individual facts and circumstances surrounding the particular vessel designated for sinking.

The final proposed legal solution for the removal of designated non-retention vessels from Suisun Bay would require a change in legislation. As discussed *supra*, foreign ship recycling is primarily frustrated by both TSCA and the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009.¹⁶³

¹⁵⁸ 40 C.F.R. § 229.2 (1977).

¹⁵⁹ *Id.*

¹⁶⁰ 33 C.F.R. § 151.2005 (1999) (as amended).

¹⁶¹ 40 C.F.R. § 229.2 (1977).

¹⁶² *Id.*

¹⁶³ Pub. L. No. 110-417, 122 Stat. 4761, § 3502 (2008).

However, the Maritime Administration continues to be approached by foreign ship recyclers to purchase its non-retention vessels.¹⁶⁴ The legislative change would require nothing more than for Congress to revert to the position it held when it promulgated the Floyd D. Spence National Defense Authorization Act of 2001,¹⁶⁵ which simply required the use of qualified scrapping facilities without predisposition toward foreign or domestic. To further ensure that foreign recycling be completed responsibly, the legislative change could also incorporate the language from the Duncan Hunter National Defense Authorization Act which requires that disposal methods be conducted in full compliance with equivalent U.S. environmental, safety, labor, and health requirements.¹⁶⁶

TSCA mandates that PCBs may not be distributed in commerce in any manner other than in a totally enclosed manner.¹⁶⁷ However, TSCA does allow an exception to this general rule for the distribution in commerce of PCBs in a manner other than in a totally enclosed manner if the EPA makes a determination that the distribution will not present an unreasonable risk of injury to health or the environment.¹⁶⁸ Many of the Reserve Fleet non-retention vessels were constructed prior to the EPA's ban on the manufacture of PCBs in 1979. As such, whether the non-retention vessels contain PCBs in a manner other than in a totally enclosed manner is always a point of contention and a source of delay in vessel disposal. To negotiate this environmental hurdle, the Maritime Administration could petition the EPA for rulemaking to authorize its ship disposal program to export all PCBs, regardless of whether the PCBs are totally enclosed. The rulemaking could be narrowly tailored by only allowing for export to developed countries and by requiring the notice to and consent of the importing country. Such a rulemaking, coupled with the proposed legislative change, would allow the Maritime Administration to contract for foreign ship recycling without being subject to delay, which would ultimately expedite the removal of all the non-retention vessels from Suisun Bay. Furthermore, because the non-retention vessels would be bound for foreign ports, the Coast Guard hull marine growth removal regulation would not apply.

¹⁶⁴ Maritime Administration's 2008 Environmental Assessment, *supra* note 46, at 2-34.

¹⁶⁵ Pub. L. No. 106-398, § 3502 (2000).

¹⁶⁶ *Id.*

¹⁶⁷ 15 U.S.C. § 2605(e)(2)(A) (1976) (as amended).

¹⁶⁸ See 15 U.S.C. § 2605(e)(2)(B) (1976) (as amended):

The Administrator may by rule authorize the manufacture, processing, distribution in commerce or use (or any combination of such activities) of any polychlorinated biphenyl in a manner other than in a totally enclosed manner if the Administrator finds that such manufacture, processing, distribution in commerce, or use (or combination of such activities) will not present an unreasonable risk of injury to health or the environment.

VII. CONCLUSION

The environmental plaintiffs are requesting the court to order the removal of all Reserve Fleet vessels from the Suisun Bay Anchorage and to enjoin the Maritime Administration from accepting any other vessels into the Suisun Bay anchorage until it is able to maintain the vessels in a manner that complies with the law.¹⁶⁹ The intervening plaintiff is requesting the court to order the Maritime Administration to comply with the CWA by either ceasing all pollutant discharges from the non-retention vessels or by acquiring the requisite NPDES permit.¹⁷⁰ The California Water Quality Board initially requested that the Maritime Administration be enjoined from engaging in any scamping, from accepting any new non-retention vessels, and from removing any non-retention vessels from Suisun Bay in violation of the CWA,¹⁷¹ but has since withdrawn those portions of its prayer for relief.¹⁷²

Now that the plaintiffs have been successful in proving the Maritime Administration's violation of environmental laws, how should the court fashion an adequate legal remedy? Surely, the court could order that the Maritime Administration not accept any other vessels into the Suisun Bay anchorage until it is able to comply with the law. But could the court order the removal of all Reserve Fleet non-retention vessels from the Suisun Bay Anchorage? As analyzed *supra*, an approved ship recycling facility does not exist in the Suisun Bay area or the entire area under the cognizance of the same Coast Guard Captain of the Port. As such, each non-retention vessel would need to have its underwater marine growth removed prior to being permitted by the Coast Guard to be towed to a recycling facility outside the area. Because the California Water Quality Board determined that the Maritime Administration's current

¹⁶⁹ First Amended Complaint, *supra* note 24, at 36.

¹⁷⁰ Complaint in Intervention, *supra* note 19, at 13.

¹⁷¹ *Id.*

¹⁷² See Plaintiff-Intervenor California Regional Water Quality Control Board's Opposition to Defendants' Motion for Partial Summary Judgment at 1-2, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Sep. 29, 2009):

With regard to threatened discharges, in light of defendants' very recent assertions that they will use dry docking as the primary method to clean the underwater portions of the hulls of SBRF non-retention vessels prior to their removal from the fleet and that they will not conduct any in-water hull cleaning without first obtaining an NPDES permit, the Regional Water Board agrees to withdraw, without prejudice, its requests for injunctive and declaratory relief concerning defendants' threatened future in-water hull cleaning and removal of non-retention vessels from the SBRF. Furthermore, in light of defendants' assertions that they will not allow new non-retention vessels into the SBRF that have exfoliated or exfoliating paint, the Regional Water Board also agrees to withdraw, without prejudice, the portion of its prayer for relief concerning the threatened future violation of allowing new non-retention vessels into the fleet that may discharge into Suisun Bay.

underwater marine growth removal method results in dissolved copper and zinc concentrations that violate California Water Quality Standards,¹⁷³ the Maritime Administration is prevented from further underwater marine growth removal.

The only remaining method to remove the hull marine growth is through the use of a dry-dock. Although the Maritime Administration represents that dry-docking is its preferred method of underwater hull cleaning for non-retention vessels,¹⁷⁴ the feasibility of dry-docking is a function of funding, vessel material readiness and dry-dock availability. The Maritime Administration understands the practicalities of competing with industry for the use of just two dry-docks in the entire San Francisco area. Furthermore, the agency believes that its non-retention vessels' weakened material integrity may not withstand the dry-dock process.¹⁷⁵ Specifically, the Maritime Administration worries that once the water is removed from the dry-dock after the vessel is floated in, the vessel's hull will fail under its own weight resulting in the vessel's inability to be floated out of the dry-dock after the marine growth removal process.¹⁷⁶ In addition, because there are currently 57 vessels in queue for disposal,¹⁷⁷ even the exclusive use of the two dry-docks and an unlimited budget would still result in the majority of the Suisun Bay non-retention vessels remaining at anchorage for the foreseeable future. Therefore, although the court could order the removal of the non-retention vessels from Suisun Bay, the Maritime Administration will be constrained in its ability to comply.

The court could also order the Maritime Administration to cease all pollutant discharges from the non-retention vessels in accordance with the CWA. However, once again it is unlikely it would be able to comply. As a result of CWA and National Invasive Species Act concerns, the Maritime Administration has only recently begun studying its long-term management strategy for its non-retention vessel fleets.¹⁷⁸ It anticipates being more discriminate in its acceptance of new vessels by requiring, *inter alia*, that hulls and topside surfaces are coated and substantially free of loose paint and that all hazardous materials not integral to the vessel are removed or accounted for.¹⁷⁹ In relation to its existing non-retention vessels, the Maritime Administration does recognize that only a minimal amount of maintenance occurs.¹⁸⁰ However,

¹⁷³ Complaint in Intervention, *supra* note 19, at 11-12.

¹⁷⁴ Maritime Administration's 2009 Environmental Assessment, *supra* note 111, at 41.

¹⁷⁵ Maritime Administration's 2008 Environmental Assessment, *supra* note 46, at 2-13.

¹⁷⁶ *Id.*

¹⁷⁷ Mar. Admin., U.S. Dep't of Transp., National Defense Reserve Fleet Inventory for the Month Ending January 31, 2010 (2010).

¹⁷⁸ Mar. Admin., U.S. Dep't of Transp., Report to Congress on the Progress of the Vessel Disposal Program 21 (2008).

¹⁷⁹ Maritime Administration's 2008 Environmental Assessment, *supra* note 46, at 2.

¹⁸⁰ *Id.* at 2-3.

in its 2008 Draft Programmatic Environmental Assessment, it discussed its intention to perform more intensive remedial actions.¹⁸¹ The remedial actions focus on testing several methods to remove the existing layers of exfoliating paint on the non-retention vessels, while at the same time recognizing that containment may prove problematic because of environmental conditions.¹⁸²

The plaintiffs' cause of action has so far resulted in the Maritime Administration's agreement not to engage in scamping any of the non-retention vessels.¹⁸³ However, the result is that the Maritime Administration is now legally prevented from disposing of any of the polluting non-retention vessels at issue in the case unless the vessels are put into dry-dock. In fact, the Maritime Administration has only been able to dispose of two Suisun Bay non-retention vessels since January of 2007.¹⁸⁴ This unintended consequence begs the question of whether the environment is better off because of the lawsuit. Although all parties may agree that the environmental laws preventing the vessel's disposal further legitimate environmental objectives, the parties may also agree that the laws were not intended to frustrate environmental progress.

Is inaction the legal remedy for this case? Would the environment be better off if the non-retention vessels sit at anchorage until technology produces a scamping method resulting in total containment of all marine growth and heavy metal discharge? Could the average cost of \$750,000¹⁸⁵ spent to dry-dock each of the remaining fifty-seven non-retention vessels for the sole purpose of removing marine growth be better spent on other environmental pursuits, such as protecting endangered species or acquiring additional species' habitat? Would the environment be better off if the Maritime Administration were allowed to keep its marine-growth laden vessels at anchorage until a local ship recycling facility is available for vessel disposal? The current reality is that after the vessels are cleaned in a San Francisco dry-dock, the vessels are towed for

¹⁸¹ *Id.* at 2-6.

¹⁸² *Id.*

¹⁸³ Joint Stipulation And Order Regarding Plaintiffs' NEPA Claims, *supra* note 29, at 2.

¹⁸⁴ See Memorandum in Support of Defendants' Motion to Stay the Litigation of Plaintiffs' First, Second, Third, and Fourth Claims for Relief at 2, *Arc Ecology v. U.S. Mar. Admin.*, No. 2:07-cv-2320-GEB-GGH (E.D. Cal. Feb. 11, 2008); see also Thomas Peele, *Mothball Fleet Being Cleaned for Ocean Voyage*, *CONTRA COSTA TIMES*, Dec. 9, 2009.

¹⁸⁵ See Mar. Admin., U.S. Dep't of Transp., DOT Deputy Secretary John D. Porcari Announces Plan to Clean Up Suisun Bay Reserve Fleet, DOT 169-09, Oct. 22, 2009:

Both ships will be cleaned at the BAE Systems San Francisco shipyard by the end of the year, and then towed to Brownsville, Texas, where they will be recycled at All Star Metals, LLC. MARAD awarded BAE Systems a \$1.47 million contract to drydock the two vessels, and ALL Star Metals a recycling contract for \$2.1 million.

forty-five days¹⁸⁶ and approximately 4800 miles to recycling facilities in the Gulf of Mexico,¹⁸⁷ resulting in significant expense, natural resource consumption and CO2 emissions.

As discussed *supra*, since the January 22, 2007, issuance of the Maritime Administration's moratorium on further ship disposal from the Suisun Bay Reserve Fleet, which directly resulted from the California Water Quality Board's position on scamping, only two non-retention vessels have been removed from Suisun Bay. In the one-year period preceding the moratorium, eight non-retention vessels were removed from the Suisun bay anchorage.¹⁸⁸ Extrapolating these same numbers for the three-year time period which has lapsed since this controversy began, approximately twenty-four of the fifty-seven remaining non-retention vessels could have been removed from Suisun Bay but for the California Water Quality Board's position on scamping. Should the additional pollution that will likely occur in Suisun Bay while funding is acquired for the dry-dock method be outweighed by the California Water Quality Board's concern over the release of dissolved copper and zinc concentrations from the scamping process?

Whether environmental progress has been frustrated by the *Arc Ecology v. U.S. Maritime Administration* litigation is debatable. However, an in-depth review of this case study leads this author to conclude that the parties' common goal of removing the non-retention vessels from Suisun Bay has certainly been hindered by the litigation. Although the plaintiffs were successful in putting the Maritime Administration on notice that its management of the Suisun Bay Reserve Fleet is unacceptable, the plaintiffs have also limited the Maritime Administration's ability to dispose of its polluting Suisun Bay non-retention vessel fleet. The litigation has also resulted in significant natural resource inefficiencies and increased CO2 emissions, as well as added substantial costs to the non-retention vessel disposal process. These additional costs for vessel disposal, coupled with the Maritime Administration's dwindling vessel disposal budget, will only increase the length of time needed to remove all the polluting non-retention vessels from Suisun Bay.¹⁸⁹

¹⁸⁶ Thomas Peele, *Mothball Fleet Being Cleaned for Ocean Voyage*, CONTRA COSTA TIMES, Dec. 9, 2009.

¹⁸⁷ Maritime Administration's 2008 Environmental Assessment, *supra* note 46, at 2-21.

¹⁸⁸ Mar. Admin., U.S. Dep't of Transp., Report to Congress on the Progress of the Vessel Disposal Program 15 (2008).

¹⁸⁹ The Maritime Administration only received \$15 million for expenses to dispose of obsolete vessels in fiscal year 2010, versus \$18 million in fiscal year 2009. See the National Defense Authorization Act for Fiscal Year 2010, Pub. L. 111-84, 123 Stat. 2190, § 3501(3) (2009); see also the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 § 3502, Pub. L. No. 110-417, 122 Stat. 4761 (2008).

TOWARD A NEW BEGINNING WITH THE INTERNATIONAL CRIMINAL COURT

Lieutenant Jeremy Snellen¹

I. INTRODUCTION

I never dreamed, at that time, that the ICC would rise to such prominence as a part of the analysis of why the United States has drifted so far from even its closest allies. One of the reasons the ICC has become so prominent is that its source treaty is emblematic of many other treaty relationships and multilateral negotiations where, in the past couple of years, the United States has disengaged rather than engaged.²

Despite consistently being a supporter of war crimes tribunals and one of the main negotiators of the treaty that created the International Criminal Court (ICC), the United States responded with hostility and obstructionism when the Rome Statute became effective in 2003. U.S. policy amounted to more than a mere refusal to become an ICC member; the United States actively sought to undermine the legitimacy of the ICC.³ In an attempt to thwart the development of the ICC, the U.S. Congress passed the American Servicemembers' Protection Act ("ASPA"). Our European allies refer to the ASPA as the "Hague Invasion Act" because it authorizes the President to use military force to prevent ICC prosecution of American servicemembers.⁴ Moreover, until recently,⁵ the ASPA imposed sanctions on countries that refused to sign bilateral agreements obligating them to shield U.S. servicemembers from ICC prosecution.⁶ The

¹ JAGC, USN. Currently stationed at Naval Legal Service Office Mid-Atlantic, Norfolk, VA. J.D., Syracuse University, 2008; M.A., Syracuse University, 2008; B.S., University of Missouri, 2005.

² Ambassador David J. Scheffer, Address at Vanderbilt University Law School: Advancing U.S. Interests with the International Criminal Court (Mar. 27, 2003), in 36 VAND. J. TRANSNAT'L L. 1567, 1567 (2003).

³ Colonel Stuart W. Risch, *Hostile Outsider or Influential Insider? The United States and the International Criminal Court*, ARMY LAW., May 2009, at 61, 66; Ron Sievert, *A New Perspective on the International Criminal Court: Why the Right Should Embrace the ICC and How America Can Use It*, 68 U. PITT. L. REV. 77, 81 (2006).

⁴ American Servicemembers' Protection Act, 22 U.S.C. §§ 7401, 7427 (2003).

⁵ On 28 January 2008, President Bush signed into law § 1212 of H.R. 4986, 110th Cong. (2008), eliminating restrictions on military assistance to nations that refused to enter into bi-lateral agreements. Moreover, the provisions of the Nethercutt Amendment, H.R. 3047, 109th Cong. (2005), which reduced economic aid to countries that refused to sign bi-lateral agreements, had all been removed or had lapsed as of early 2009.

⁶ 22 U.S.C. § 7426 (2003) (repealed 2008).

ASPA also significantly restricts U.S. cooperation with the ICC.⁷ U.S. agencies may only cooperate with the ICC as to specific people or issues, and in those cases only if the President issues waivers and follows certain notification procedures.⁸ The United States and Turkey are the only NATO members who have not joined the ICC.⁹ More significantly, the United States is the only democracy that has sought to undermine the ICC. Other democracies are nearly unanimous in their desire to see the ICC develop into an institution that improves global justice and stability.¹⁰

The Obama Administration has signaled its intent to change the foreign policy of the previous administration. In a speech in Cairo in June 2009, President Obama addressed many of the challenges facing the United States and the international community. Confronting violent extremism, easing the tension between the Israelis and Palestinians, and fostering democracy and women's rights around the world are but a few of those challenges. However, a new beginning requires more than words, and "no single speech can eradicate years of mistrust."¹¹ If the United States truly wants to signal a new beginning, it must engage in reforms and initiatives that demonstrate to the international community that U.S. foreign policy priorities have been reordered. The U.S. policy toward the ICC represents an area where new beginnings could be demonstrated.

The Obama Administration is gradually adopting a more cooperative approach toward the ICC. In furtherance of this new approach, the United States is sending a delegation to observe the ICC Review Conference scheduled for the summer of 2010. As the U.S. official made the announcement, he noted, "We are certainly looking to engage with the ICC to ensure where there are no other avenues for accountability, that it will be an effective instrument for ensuring that individuals are brought to justice."¹² Although observing ICC meetings is a positive step, true cooperation requires something more. It is unclear how much the United States can participate in the ICC Review Conference given the current anti-ICC laws in force.¹³ An institutionalized and

⁷ Cooperation includes assistance such as financial support, legal services, intelligence sharing, law enforcement cooperation, and expertise contributions. The United States has consistently provided this kind of cooperation to other international war crimes tribunals.

⁸ 22 U.S.C. §§ 7422-7424 (2003).

⁹ For a list of States Parties to the ICC, see International Criminal Court, <http://www.icc-cpi.int/Menus/ASP/states+parties/> (last visited Feb. 15, 2010).

¹⁰ Risch, *supra* note 3, at 74-75; Sievert, *supra* note 3, at 81.

¹¹ President Barak Obama, Remarks at Cairo University: On a New Beginning (June 4, 2009).

¹² Interview by reporters with Stephen Rapp, U.S. Ambassador-at-Large for War Crimes Issues on BBC News (Nov. 16, 2009).

¹³ The American Society of International Law, Independent Task Force, U.S. POLICY TOWARD THE INTERNATIONAL CRIMINAL COURT: FURTHERING POSITIVE ENGAGEMENT 33 (2009) [hereinafter ASIL Independent Task Force Report].

systematic program of cooperation by the United States will require the repeal of ASPA.¹⁴

U.S. cooperation with the ICC could allow the institution to develop and help the United States enhance its moral authority and global credibility. U.S. obstructionism has been the single biggest impediment to the development of the ICC.¹⁵ Few recent U.S. policy decisions, save for possibly the Iraq intervention and the treatment of alleged terrorist detainees, have created as much global resentment toward the United States.¹⁶ This deep resentment weakens U.S. national security by making it more difficult to defend the legitimacy of military operations abroad, increasing the appeal of radical anti-Americanism to vulnerable individuals, and making it more difficult to build support amongst other countries for U.S. foreign policy initiatives.¹⁷

This article attempts to address the concerns of the U.S. opponents of the ICC. These concerns are straightforward and all revolve around the potential exposure of U.S. servicemembers to ICC prosecution.¹⁸ This is a legitimate concern that should be analyzed carefully. However, a good portion of criticism by opponents in the United States relies on unlikely hypotheticals and a failure to fully appreciate protections provided by the ICC. The article also recommends that the Obama Administration take more substantive steps to cooperate with the ICC. Finally, it explains why the Department of Defense (“DoD”) should support this policy shift toward cooperation. This article does not advocate that the United States become an ICC State Party at this time. Rather, it proposes an interim cooperative stance, which will benefit both the ICC and the United States.

This article proceeds in three sections. Section One explains the ICC protections that make it unlikely that U.S. servicemembers will be subjected to ICC prosecution. Section Two tackles the controversy head-on by addressing several hypothetical situations where U.S. servicemembers could come under ICC scrutiny. The ICC protections explained in Section One are applied to these hypotheticals in order to illustrate the obstacles in place to the prosecution of a U.S. servicemember by the ICC. Section Three discusses policy implications

¹⁴ *Id.*

¹⁵ Risch, *supra* note 3, at 80-83, 87; Kenneth Roth, Remarks at the University of Oregon School of Law: Human Rights as a Response to Terrorism (Feb. 11, 2004), in 6 OR. REV. INT'L L. 37, 57-58 (2004); Michael P. Hatchell, Note, *Closing the Gaps in United States Law and Implementing the Rome Statute: A Comparative Approach*, 12 ILSA J. INT'L & COMP. L. 183, 211 (2005).

¹⁶ Risch, *supra* note 3, at 66; Roth, *supra* note 15, at 57-61.

¹⁷ Risch, *supra* note 3, at 80-83, 89; Roth *supra* note 15, at 53-61; Allen J. Dickenson, *Who's in Charge Here?—International Criminal Court Complementarity and the Commander's Role in Courts Martial*, 54 NAVAL L. REV. 141, 158 (2007).

¹⁷ Risch, *supra* note 3, at 75; Roth, *supra* note 15, at 55.

and argues that cooperation with the ICC is beneficial to confronting radical extremism and strengthening U.S. national security.

II. ICC PROTECTIONS AGAINST THE PROSECUTION OF U.S. SERVICEMEMBERS

The United States was a main negotiator in the drafting of the Rome Statute and succeeded in gaining inclusion of comprehensive protections.¹⁹ In fact, the United States was granted nearly every concession it sought except an iron-clad exemption of U.S. servicemembers from prosecution.²⁰ Notwithstanding the lack of such an iron-clad exemption, the comprehensive protections, particularly when analyzed alongside several practical considerations, make it very difficult for the ICC to prosecute U.S. servicemembers. These protections are organized as follows: (A) types of crimes; (B) jurisdictional ICC limitations; (C) U.N. Security Council (UNSC) oversight; and, (D) procedural protections inherent in the Rome Statute.

A. ICC Protections Based on Types of Crimes

The ICC only has authority to prosecute three types of crimes, and the U.S. government is simply not in the business of conspiring to commit genocide, crimes against humanity, or war crimes.²¹ The United States places a strong impetus on its servicemembers obeying the laws of war.²² Despite rigorous selection and training, some U.S. servicemembers require discipline, and when violations occur they are disciplined under the Uniform Code of Military Justice (UCMJ).²³ The Rome Statute's preamble makes clear that the ICC is only concerned with grave and serious "crimes that threaten the peace, security, and well-being of the world."²⁴ The Rome Statute incorporates this ideal into its substantive provisions.

¹⁸ Sievert, *supra* note 3, at 110-129; *see generally* Scheffer, *supra* note 2.

¹⁹ Risch, *supra* note 3, at 75; Roth, *supra* note 15, at 55.

²⁰ Scheffer, *supra* note 2, at 1569; U.S. DEP'T OF DEFENSE, DIR. 2311.01E, DoD LAW OF WAR PROGRAM para. 4 (9 May 2006) [hereinafter DoD Law of War Directive]; U.S. DEP'T OF ARMY AND U.S. MARINE CORPS, FIELD MANUAL 3-24, COUNTERINSURGENCY 347-361 (22 Jan. 2007) [hereinafter Army and Marine Corps Counterinsurgency Manual].

²¹ DoD Law of War Directive, *supra* note 21, at para. 4; Army and Marine Corps Counterinsurgency Manual, *supra* note 21, at 351-357; INT'L & OPERATIONAL LAW DEP'T, THE JUDGE ADVOCATE GENERAL'S LEGAL CENTER & SCHOOL, U.S. ARMY, JA 422, OPERATIONAL LAW HANDBOOK 49-104 (2008) [hereinafter JAG Operational Law Handbook].

²² DoD Law of War Directive, *supra* note 21, at para. 4; U.S. Army and Marine Corps Counterinsurgency Manual, *supra* note 21, at 351-357; JAG Operational Law Handbook, *supra* note 22, at 49-104.

²³ Sievert, *supra* note 3, at 110; Rome Statute of the International Criminal Court Preamble, July 17, 1998, 37 I.L.M. 1002 (effective July 1, 2002) [hereinafter Rome Statute].

Genocide can be prosecuted under the Rome Statute if committed with intent to destroy a particular group of individuals.²⁵ The elements of genocide are not satisfied by the killing of one individual or even a few individuals. The U.S. government is not going to attempt to eliminate or reduce members of a national, racial, ethnic or religious group.²⁶

Crimes against humanity must be committed as part of a widespread or systematic attack against a civilian population.²⁷ As in the case of genocide, the intent element is dispositive. These crimes require multiple commissions of acts “pursuant to or in furtherance of a State or organizational policy to commit such attack.”²⁸ The United States does not have any policy that encourages servicemembers to direct attacks against civilian populations. Accordingly, no actions by U.S. servicemembers could legitimately be construed as crimes against humanity.²⁹

War crimes under the Rome Statute merit more analysis. War crimes are defined as grave breaches of the Geneva Conventions and other serious violations of international humanitarian law, in particular when committed as part of a plan or policy or on a large scale. Scholars and government officials disagree about the legal significance of the “in particular” language.³⁰ At the very least, the limitation is ambiguous. If the ICC ever initiates a formal investigation of U.S. servicemembers, it will probably be for an alleged war crimes violation.

Opponents of the ICC, within DoD or otherwise, ground their arguments in a hypothetical war crimes prosecution. They assert that the ICC will utilize this mechanism to second-guess the decisions of commanders in the field, and U.S. political adversaries will use the ICC as a tool to counter U.S. power. However, DoD policy has long emphasized U.S. obligations under the Geneva Conventions, as well as other applicable treaties and customary

²⁴ Rome Statute, *supra* note 24, at art. 6.

²⁵ DoD Law of War Directive, *supra* note 21, at para. 4; U.S. Army and Marine Corps Counterinsurgency Manual, *supra* note 21, at 347-361; JAG Operational Law Handbook, *supra* note 22, at 49-104.

²⁶ Rome Statute, *supra* note 24, at art. 7.

²⁷ International Criminal Court Elements of Crimes, art. 7 Introduction, Sept. 9, 2002, *available at* http://www.icc-cpi.int/NR/rdonlyres/9CAEE830-38CF-41D6-AB0B-68E5F9082543/0/Element_of_Crimes_English.pdf [hereinafter ICC Elements of Crimes].

²⁸ DoD Law of War Directive, *supra* note 21, at para. 4; U.S. Army and Marine Corps Counterinsurgency Manual, *supra* note 21, at 347-361; JAG Operational Law Handbook, *supra* note 22, at 49-104.

²⁹ Dickenson, *supra* note 17, at 145-146, 149.

international law.³¹ In addition, as will be explained in subsequent sections, many other ICC safeguards exist.

In the interest of completion, it is important to note that the crime of aggression is not yet incorporated into the Rome Statute. Though provisions are in place to define and incorporate aggression into an actionable ICC crime, it is not likely to happen in the near future.³² Seven-eighths of States Parties must agree upon and then ratify an amendment defining the crime of aggression.³³ And even if this crime is added in the future, new members to the Rome Statute can choose not to be bound by it.³⁴

B. Jurisdictional Limitations on ICC Prosecution

The issue of jurisdiction under the Rome Statute is divided into two subsets: Preconditions to jurisdiction and the exercise of jurisdiction.³⁵ Provisions relating to the former prescribe where, and against whom, the ICC can exercise jurisdiction. Provisions relating to the latter prescribe how, and by whom, ICC jurisdiction can be triggered. As a preliminary note, the ICC can only exercise jurisdiction over crimes committed after July 2002, when the Rome Statute became effective, and new members can opt out of ICC jurisdiction over any crimes that occurred before they acceded to the treaty.³⁶

The preconditions include the limitation of ICC jurisdiction to States Parties.³⁷ In other words, the alleged crime must have occurred on the territory of a State Party or have been committed by a national of a State Party. There are a couple of exceptions to this general rule. First, a UNSC referral confers universal jurisdiction. For example, in the case of the 2005 Darfur referral, Sudan was not a State Party, but jurisdiction flowed from UNSC authorization.³⁸ Second, a Non-State Party may accept the jurisdiction of the ICC for a particular crime or case.³⁹ Because of the permanent status of the United States on the

³⁰ JAG Operational Law Handbook, *supra* note 22, at 49-104; DoD Law of War Directive, *supra* note 21, at para. 3 (“The law of war encompasses all international law for the conduct of hostilities binding on the United States or its individual citizens, including treaties and international agreements to which the United States is a party, and applicable customary international law”).

³¹ Scheffer, *supra* note 2, at 1569-1575.

³² Rome Statute, *supra* note 24, at arts. 121, 123.

³³ Scheffer, *supra* note 2, at 1575.

³⁴ Rome Statute, *supra* note 24, at arts. 12-13.

³⁵ *Id.* at art. 11.

³⁶ *Id.* at art. 12.

³⁷ S.C. Res. 1593, U.N. Doc. S/Res/1593 (March 31, 2005) (with the United States abstaining from voting).

³⁸ Rome Statute, *supra* note 24, at art. 12; Lieutenant Commander Gregory P. Noone & Douglas William Moore, *An Introduction to the International Criminal Court*, 46 NAVAL L. REV. 112, 151

UNSC, the first exception does not render the prosecution of U.S. servicemembers any more likely. The second exception, however, which allows a Non-State Party to accept jurisdiction of the ICC for a particular crime occurring in its territory, is a source of greater concern and is likely the precondition that would be utilized if a U.S. servicemember were to be formally investigated.

Turning to the exercise of jurisdiction, there are three methods.⁴⁰ Two are not controversial, but one has prompted protests from the United States. The first method is UNSC referral. Though this method does not have the preconditional limitations of the other two, it has not generated controversy because the United States can veto any referral of a case involving a U.S. servicemember. The second method is the referral of a case by a State Party. The preconditions apply fully to this method as they do to the third. Accordingly, the alleged crime must have occurred in the territory of the State Party or have been committed by a national of the State Party. The third method of exercising jurisdiction is referral by the ICC prosecutor. It is this third and last method that has generated the most controversy because the United States believes the Rome Statute confers too much discretion on the ICC prosecutor.

Although prosecutorial referral is controversial, it has its own unique safeguards, which are often overlooked.⁴¹ Under the Rome Statute, the prosecutor cannot initiate a formal investigation without the authorization of the ICC Pre-Trial Chamber.⁴² Moreover, before the prosecutor submits the matter to the Pre-Trial Chamber, he or she must conduct a preliminary inquiry and make the following determinations: (a) Whether the available evidence provides a reasonable basis to believe the alleged crime has been committed within the jurisdiction of the court; (b) Whether the case would be admissible in light of the requirements of gravity and complementarity; and, (c) Whether the interests of justice would be served by an investigation.⁴³ Complementarity requires notification to the State(s) that would normally have jurisdiction to prosecute and the provision of ample opportunity for that State to investigate the matter.⁴⁴ Only if all these preliminary determinations are resolved in favor of proceeding

(1999); *see also*, Ruth Wedgewood, *Fiddling in Rome: America and the International Criminal Court*, 77(6) FOREIGN AFF. 20 (1998).

³⁹ Rome Statute, *supra* note 24, at art. 13.

⁴⁰ Rome Statute, *supra* note 24, at art. 15; Sievert, *supra* note 3, at 111; *see generally* Scheffer, *supra* note 2.

⁴¹ Rome Statute, *supra* note 24, at art. 15.

⁴² *Id.*; *see also* Letter from Luis Moreno-Ocampo, Chief Prosecutor of the International Criminal Court, in response to 240 communications concerning Iraq (Feb. 9, 2006), *available at* http://www.icc-cpi.int/NR/rdonlyres/04D143C8-19FB-466C-AB77-4CDB2FDEBEF7/143682/OTP_letter_to_senders_re_Iraq_9_February_2006.pdf [hereinafter Ocampo Iraq Communication].

⁴³ Rome Statute, *supra* note 24, at art. 18.

may the prosecutor submit the matter to the Pre-Trial Chamber for review. This body, not the prosecutor, decides whether to initiate the formal investigation.

Even an initial decision by the Pre-Trial Chamber to formally investigate does not preclude a later determination that the case is inadmissible because, for example, the ICC lacks jurisdiction or the alleged crimes do not have sufficient gravity.⁴⁵ Furthermore, before any investigation commences, the State involved can appeal the decision of the Pre-Trial Chamber to the ICC Appellate Chamber, which would have to approve the investigation.⁴⁶ Finally, as explained below, the UNSC can defer any investigation indefinitely.

C. UNSC Oversight

The UNSC can defer any ICC investigation by adopting a resolution that such investigation would be harmful to global peace and security.⁴⁷ The UNSC can renew this deferral annually, with no limitation on the number of renewals.⁴⁸

If the United States had a more cooperative stance toward the ICC, it could use its permanent status on the UNSC to influence the agenda of the ICC and, if necessary, defer an investigation of a U.S. servicemember indefinitely.⁴⁹ If the United States used its status and credibility to defer an investigation, only a veto from another permanent member could block the deferral. Russia and China are both hostile toward the ICC. Britain and France are two of the strongest allies of the United States. Under these circumstances, UNSC oversight is a powerful instrument the United States could use to influence the agenda of the ICC.

D. Procedural Protections Encompassed in the Rome Statute

The U.S. negotiators fought for and were able to incorporate stringent admissibility and procedural protections into the Rome Statute.⁵⁰ Two admissibility prerequisites—complementarity and gravity—ensure that the ICC will only try the most serious crimes and only when States that would normally exercise jurisdiction are unwilling or unable. Moreover, assuming the initiation of a formal investigation, an accused individual receives due process protections similar to those found in our Constitution.⁵¹ For example, the Rome Statute

⁴⁴ *Id.* at art. 15.

⁴⁵ *Id.* at art. 19.

⁴⁶ *Id.* at art. 16; *see also* Noone & Moore, *supra* note 39, at 143.

⁴⁷ Rome Statute, *supra* note 24, at art. 16; Noone & Moore, *supra* note 39, at 143.

⁴⁸ Scheffer, *supra* note 2, at 1575.

⁴⁹ *Id.* at 1571-1572; *see also* Sievert, *supra* note 3, at 113-114.

⁵⁰ Scheffer, *supra* note 2, at 1571-1572; Sievert, *supra* note 3, at 113-114.

confers a presumption of innocence upon the accused, a privilege against self-incrimination, and the right to confrontation of witnesses and the disclosure of exculpatory evidence.⁵² Arguably, the procedural protections are even more comprehensive and detailed than in the U.S. justice system.⁵³ The admissibility prerequisites are most significant for U.S. purposes—they make it difficult for a State or group to cause an investigation of a U.S. servicemember to ever go forward.

That said, the ICC is intended to complement, not supplant, State criminal justice systems.⁵⁴ A case is inadmissible if the complementarity prong is not satisfied. In other words, if a State, whether Party or Non-Party, has conducted an investigation and either prosecuted or determined prosecution is unwarranted, then the case is inadmissible.⁵⁵ As mentioned previously, before any investigation proceeds, the prosecutor must notify the State(s) that would normally have jurisdiction and give the State the opportunity to investigate.⁵⁶ If the State responds that it is investigating the matter, then the prosecutor must defer to the State.

The Rome Statute does provide a means to pierce the complementarity shield to prevent States from hiding behind it and rendering the ICC powerless. To pierce the complementarity shield, the Pre-Trial Chamber must determine that the State proceedings (a) merely constitute an attempt to shield someone from criminal responsibility; (b) represent an unjustifiable delay inconsistent with due process; or (c) were not conducted independently by State institutions.⁵⁷ This ruling is appealable to the Appellate Chamber on an expedited basis. The ICC will rarely pierce the complementarity shield, but the prospect gives the ICC the necessary power to be effectual.⁵⁸ The government of Sudan and the conflict in Darfur constitute a perfect example of why this power is essential.⁵⁹ The ICC is powerless unless it can enforce justice upon rogue, criminal regimes.

Gravity is the other significant ICC admissibility prerequisite.⁶⁰ The ICC is not interested in prosecuting small scale crimes by individual soldiers—its interest lies in serious crimes that affect international peace and security. The

⁵¹ Rome Statute, *supra* note 24, at arts. 62-76.

⁵² Scheffer, *supra* note 2, at 1571-1572; Sievert, *supra* note 3, at 113-114.

⁵³ Scheffer, *supra* note 2, at 1572-1573; Risch, *supra* note 3, at 71; Noone & Moore, *supra* note 39, at 140-141.

⁵⁴ Rome Statute, *supra* note 24, at arts. 17, 18.

⁵⁵ *Id.* at art. 18.

⁵⁶ *Id.* at art. 17.

⁵⁷ Scheffer, *supra* note 2, at 1573.

⁵⁸ Risch, *supra* note 3, at 73-74.

⁵⁹ Rome Statute, *supra* note 24, at art. 17(d).

ICC gravity precedent is beginning to take shape.⁶¹ During the height of the Iraq conflict, several groups attempted to persuade the ICC prosecutor to initiate an investigation into alleged prisoner abuse by British troops. ICC Prosecutor Moreno-Ocampo stated that even if there were a reasonable basis to believe that a crime within the ICC's jurisdiction had occurred, the allegations would not warrant an investigation because the number of potential victims did not satisfy the gravity prerequisite when compared with the atrocities in Uganda, the Democratic Republic of Congo, and the Sudan.⁶²

Lastly, consider the necessary qualifications and oversight of ICC judges and prosecutors. They are elected by States Parties for a fixed, nine-year term.⁶³ The Rome Statute mandates that judges and prosecutors possess the qualifications required in their respective States for appointment to the highest judicial offices, and they must have established competency in criminal law, criminal procedure, and international law.⁶⁴ No two judges can be from the same State, and the prosecutor and deputy prosecutor cannot be from the same State.⁶⁵ Judges and prosecutors must remain impartial and professional throughout their tenure or be subject to removal.⁶⁶ Judges can be removed by a majority vote of the remaining judges.⁶⁷ Prosecutors can be removed by a majority vote of the Appeals Chamber.⁶⁸ The ICC's nexus of procedural safeguards, oversight, and judicial qualifications provide a bulwark against exploitation of the court for political ends.

III. HYPOTHETICALS WHERE U.S. SERVICEMEMBERS COULD BE SCRUTINIZED BY THE ICC

Since much of the U.S. criticism of the ICC focuses on hypotheticals that imagine a U.S. servicemember on trial in The Hague, hypotheticals will be a central focus of this article. Each relying on several foundational assumptions, these hypotheticals represent the most likely chain of events which could lead to a U.S. servicemember being the subject of ICC scrutiny. The main foundational assumption for each, and a significant one at that, will be a predetermined jurisdictional platform that brings U.S. servicemembers under

⁶⁰ Ocampo Iraq Communication, *supra* note 43; Alexander K.A. Greenawalt, *Justice Without Politics? Prosecutorial Discretion and the International Criminal Court*, 39 N.Y.U. J. INT'L L. & POL. 583, 641 (2007).

⁶¹ The groups alleged between four and twelve individuals were willfully killed and fewer than twenty subjected to inhumane treatment.

⁶² Rome Statute, *supra* note 24, at art. 36.

⁶³ *Id.*

⁶⁴ *Id.* at arts. 36, 42.

⁶⁵ *Id.*

⁶⁶ *Id.* at art. 36.

⁶⁷ Rome Statute, *supra* note 24, at art. 42.

ICC authority. From there, the hypotheticals walk through the steps the ICC would likely take and the protections that would likely prevent the prosecution of a U.S. servicemember in The Hague. Finally, the article will explain why, even if one of these hypotheticals or a variation thereon allowed the ICC to legitimately consider prosecuting a U.S. servicemember, the ICC would be unlikely to act.

A. Haditha-Type Incident and Iraq Consents to ICC Jurisdiction

Assume numerous servicemembers are killed when an improvised explosive device (IED) explodes amidst a U.S. convoy operating in Iraq. Emotions overpower restraint, and several U.S. servicemembers retaliate against a group of nearby civilians. The incident is exposed to the global media, and both the governments of Iraq and the United States come under intense pressure to hold the servicemembers accountable. Iraq is not a State Party to the Rome Statute. So, how could the ICC possibility get involved?

Assume further that Iraqi leadership has changed, and Iraq is no longer amenable to a U.S. military presence. Iraqi leaders are dissatisfied with the slow pace of the U.S. military justice system and decide they are not bound by the Status of Forces Agreement (“SOFA”). In the face of pressure from their constituents, they consent to ICC jurisdiction ad hoc for this particular incident. Several Iraqi nongovernmental groups and nongovernmental organizations from other States collect evidence and send it to the ICC prosecutor, requesting the initiation of a formal investigation. This jurisdictional platform is within the realm of the possible. How would this situation be treated by the ICC?

As noted earlier, before the prosecutor could initiate any formal investigation, he or she would need to obtain the authorization of the ICC Pre-Trial Chamber. Before submitting the matter to the Pre-Trial Chamber, the prosecutor must take several preliminary steps, and then get authority from the Pre-Trial Chamber.⁶⁹ The prosecutor would have to make the following preliminary determinations: (a) whether the available evidence provided a reasonable basis to believe the alleged crime had been committed within the jurisdiction of the court; (b) whether the case would be admissible in light of the requirements of gravity and complementarity; and, (c) whether the interests of justice would be served by an investigation.⁷⁰

The ICC prosecutor would not present the situation to the Pre-Trial Chamber because the admissibility requirements would not be met. The key

⁶⁸ *Id.* at art. 15.

⁶⁹ *Id.* at art. 15; Ocampo Iraq Communication, *supra* note 43, at 2.

component of the gravity analysis is the number of victims.⁷¹ Here, there would be at most 10-15 civilian victims. When compared with the other ongoing ICC investigations in Uganda, the Democratic Republic of Congo, and Darfur, in which hundreds of thousands of civilians are alleged to have been killed, in our situation the gravity threshold is not met. Even assuming the complementarity analysis would be considered, though it is not necessary without sufficient gravity,⁷² it would also not be satisfied because the U.S. is more aggressive than most developed nations in holding servicemembers accountable when they cross the line of impermissible conduct.⁷³ An investigation would be underway and ample information about the pending investigation would be public. As a reminder, an investigation followed by a decision that prosecution is not warranted still renders a case inadmissible.⁷⁴ Complementarity can only be pierced if no investigation is done at all or a farcical investigation is conducted.⁷⁵

A real-life variation of this hypothetical occurred and the ICC prosecutor declined to recommend a formal investigation.⁷⁶ As briefly mentioned earlier, in 2006 at the height of the Iraq war's unpopularity, the current ICC prosecutor, Luis Moreno-Ocampo, responded to the receipt of over 240 submissions by public and private entities.⁷⁷ The organizations urged the prosecutor to initiate an investigation of coalition forces for alleged crimes ranging from willful killing to inhuman treatment and even the use of cluster munitions.⁷⁸ Jurisdiction was at least plausible because British troops were involved in some of the alleged incidents, and the United Kingdom is a State Party. The prosecutor found that the evidence provided a reasonable basis to believe that crimes were committed.⁷⁹ However, in less than one page of analysis, he determined the matter to be inadmissible because it was not of sufficient gravity and, moreover, "national proceedings had been initiated with respect to each of the relevant incidents."⁸⁰

⁷⁰ *Ocampo Iraq Communication*, *supra* note 43, at 8-9.

⁷¹ *Id.* at 9.

⁷² Risch, *supra* note 3, at 88 (citing the DoD Law of War Directive); JAG Operational Law Handbook, *supra* note 22, at 49-104.

⁷³ Rome Statute, *supra* note 24, at art. 17.

⁷⁴ *Id.*

⁷⁵ *See generally* Ocampo Iraq Communication, *supra* note 43; *see also* Risch, *supra* note 3, at 77.

⁷⁶ *See generally* Ocampo Iraq Communication, *supra* note 43.

⁷⁷ *Id.* at 4-10.

⁷⁸ *Id.* at 8.

⁷⁹ *Id.* at 8-9.

B. Airstrike Causing Civilian Deaths and a Reneging Afghan Government

Assume a predator drone strike targets high-value Al Qaeda operatives in southern Afghanistan, but the operatives evade the strike, and fifty civilians are killed instead. Prior to conducting the strike, the United States knew that some civilians would be present but ordered the strike based on a determination that the opportunity to eliminate these operatives warranted the risk to civilian lives. Next, assume that Afghanistan, as a State Party to the Rome Statute, reneges on its SOFA with the United States and refers the situation to the ICC. This jurisdictional platform, or a variation of it, is at least plausible. How would this situation be treated by the ICC?

Though initiation of the investigation will not require Pre-Trial Chamber authorization due to its referral by a State Party, the prosecutor still must take similar preliminary steps. The U.S. will be allowed the opportunity to investigate and decide whether the situation warrants criminal prosecution. The prosecutor still must determine if a reasonable basis for the charges exists and whether the case will be admissible.⁸¹ At some time thereafter, unless the prosecutor has not already ceased the investigation, the ICC Trial Chamber will undertake an admissibility determination either on motion of a party to the case, or if need be on its own motion.⁸²

The airstrike scenario would not result in U.S. servicemembers standing trial in The Hague. Lack of reasonable basis, or of gravity, or of complementarity, or a combination of all these preliminary determinations would mandate that the situation be set aside. Under the Rome Statute Article 8(2)(b)(iv), which incorporates the Geneva Conventions definition, in order to be criminal an airstrike would have to be characterized as:

Intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated.⁸³

⁸⁰ Rome Statute, *supra* note 24, at art. 15; Press Release, ICC Office of the Prosecutor, The Prosecutor of the ICC opens investigation in Darfur, ICC-OTP-0606-104 (July 6, 2005) (the prosecutor must undergo this preliminary inquiry even where a situation is referred by UNSC).

⁸¹ Rome Statute, *supra* note 24, at art. 17.

⁸² *Id.* at art. 8(2)(b)(iv).

U.S. Rules of Engagement (“RoE”) have long emphasized all of these core concepts—only striking legitimate military targets and minimizing incidental loss of life.⁸⁴ In determining whether to undertake an airstrike against a terrorist target, U.S. commanders and their JAG advisors thoroughly analyze the military advantages and the potential harm to civilians.⁸⁵ If an engagement decision is not conducted correctly, or the loss of civilian life is clearly excessive to the anticipated military advantage, then the U.S. will investigate. As such, when U.S. commanders decide to launch an airstrike against terrorist targets, there is no opening for the ICC to question their judgment.

Real life variations of this hypothetical have taken place. During NATO’s intervention in the former Yugoslavia, airplanes launched a missile attack on the headquarters of the Federal Republic of Yugoslavia’s state-owned TV and radio company, killing sixteen civilians inside and damaging the building.⁸⁶ NATO planes had intentionally bombed the structure knowing civilians were present following a determination by NATO commanders that any incidental loss of life would be proportionate to the military advantage.⁸⁷ The prosecutor for the International Criminal Court of the Former Yugoslavia created a special U.N. committee to review this incident and other alleged war crimes committed by NATO forces.⁸⁸ The committee applied a test identical to the reasonable basis test set forth in the Rome Statute and determined that the civilian deaths, while unfortunately high, were not clearly excessive.⁸⁹ The U.N. committee decided against recommending an investigation even though “NATO ha[d] admitted that mistakes did occur during the bombing campaign; errors of judgment may also have occurred.”⁹⁰

An even more revealing example can be found in the previously mentioned ICC communication concerning the situation in Iraq, in which the prosecutor conducted this analysis with regard to the bombing during the March-May 2003 Iraq invasion.⁹¹ The prosecutor did not even reach the gravity

⁸³ JAG Operational Law Handbook, *supra* note 22, at 73-104; Army and Marine Corps Counterinsurgency Manual, *supra* note 21, at 347-361.

⁸⁴ JAG Operational Law Handbook, *supra* note 22, at 73-104; Risch, *supra* note 3, at 88; Colonel Kelly D. Wheaton, *Strategic Lawyering: Realizing the Potential of Military Lawyers at the Strategic Level*, ARMY LAW., Sep. 2006, at 1.

⁸⁵ Greenawalt, *supra* note 61, at 635; United Nations, the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, Final Report to the Prosecutor, paras. 71-79, (June 13, 2000), available at <http://kosova.org/post/UN-Final-Report-to-the-NATO-Bombing-Campaign-Against-Yugoslavia.aspx> [hereinafter U.N. Review of NATO Bombing].

⁸⁶ U.N. Review of NATO Bombing, *supra* note 86, at para. 71.

⁸⁷ Greenawalt, *supra* note 61, at 635.

⁸⁸ U.N. Review of NATO Bombing, *supra* note 86, at paras. 71, 79.

⁸⁹ *Id.* at para. 90.

⁹⁰ Ocampo Iraq Communication, *supra* note 43, at 4-7.

and complementarity analyses because he found no reasonable basis for believing crimes had occurred.⁹² The prosecutor noted that lists of potential targets were identified in advance; commanders received continuous legal advice on proportionality and distinction; detailed computer modeling was used in assessing targets; and nearly eighty-five percent of the weapons released by U.K. aircraft were precision-guided.⁹³ He made special note that the criminal prohibition under Article 8(2)(b)(iv) of the Rome Statute is restricted to cases that are “clearly” excessive. The prosecutor concluded his brief analysis by stating that “the resulting information did not allow for the conclusion that there was a reasonable basis to believe that a clearly excessive attack within the jurisdiction of the Court had been committed.”⁹⁴

C. A Rogue Nation Attempts to Use the ICC as a Political Instrument Against the United States

Assume North Korea arrests three U.S. journalists for alleged espionage and trespassing. It is unclear whether the journalists were in North or South Korean territory when arrested. Diplomatic negotiations fail and, to prevent their execution, the United States frees the journalists in a special military operation. The operation succeeds, but five North Koreans, two civilian government employees, and three soldiers are killed by U.S. special forces. North Korea ad hoc accepts ICC jurisdiction, and it persuades a State Party such as Venezuela to refer the matter to the ICC. The rogue nations allege willful killing; extensive destruction and appropriation of property; clearly excessive incidental death of civilians; using diplomats in a perfidious attempt to conceal the rescue mission; and violation of an established demilitarized zone. How would the ICC treat this situation?

It is unlikely this situation would lead to a formal investigation. Again, the prosecutor would need to determine whether there was a reasonable basis to believe that any of the alleged crimes had occurred, whether the requirements of gravity and complementarity had been satisfied, and whether a prosecution would serve the interests of justice.⁹⁵ Hence, even if a reasonable basis exists, sufficient gravity is established, and complementarity does not eliminate the situation, the prosecutor can still decline to investigate if “there are nonetheless substantial reasons to believe that an investigation would not serve the interests of justice.”⁹⁶ A determination of the interests of justice would require consideration of factors such as the number of victims, the interests of the

⁹¹ *Id.*

⁹² *Id.* at 6-7.

⁹³ *Id.* at 7.

⁹⁴ Rome Statute, *supra* note 24, at art. 15.

⁹⁵ *Id.* at art. 53.

victims, the impact of the crimes on peace and security, and a reemphasis that the ICC is concerned with only the most serious of international crimes.⁹⁷

Here the current ICC prosecutor, and most likely subsequent ones as well, declines to throw the ICC into this heated political quarrel. Assume a reasonable basis is found for at least one of the alleged crimes, though bear in mind this would not preclude a host of defenses at later stages which would probably defuse criminal culpability. The U.S. undertakes comprehensive legal and ethical analysis before ordering any type of special military operation.⁹⁸ Only five people died in the attack. Three were soldiers who captured and held civilian prisoners under questionable pretenses. The victims all work for an army which probably engages in more human rights abuses than any other in the world. Taking the totality of circumstances into account, specifically the ongoing ICC investigations in war-torn African countries in which hundreds of thousands of civilians are alleged to have been killed, the prosecutor likely decides to focus resources on situations which the ICC was created to alleviate.

Moreover, if this unlikely chain of events did indeed lead to a formal ICC investigation, the United States could use its UNSC permanent status to indefinitely defer the investigation.⁹⁹ The only possible obstacle to this course of action would be a veto by one of two strong U.S. allies, France and Britain, or by one of two nations opposed to the ICC, China and Russia.

D. The United States Should Not Be Scared of Hypotheticals

These hypotheticals illustrate that it is unlikely a U.S. servicemember will ever stand trial in The Hague. While the United States remains a Non-State Party, the ICC does not have jurisdiction over U.S. territory and is unlikely to gain jurisdiction over U.S. servicemembers. Even if some combination of circumstances allowed for ICC jurisdiction over a U.S. servicemember, the prosecutor would have to find a reasonable basis to proceed. The United States places a strong impetus on preventing its servicemembers from conducting operations which could be construed as war crimes, genocide, or crimes against humanity.¹⁰⁰ If these crimes are ever committed by U.S. servicemembers, the

⁹⁶ International Criminal Court Office of the Prosecutor, Policy Paper on the Interests of Justice, Ref-ICC-OTP-InterestsOfJustice, 4-9 (Sept. 2007), available at: <http://www.icc-cpi.int/NR/rdonlyres/772C95C9-F54D-4321-BF09-73422BB23528/143640/ICCOTPInterestsOfJustice.pdf>.

⁹⁷ JAG Operational Law Handbook, *supra* note 22, at 73-104; Risch, *supra* note 3, at 88; Wheaton, *supra* note 85.

⁹⁸ Rome Statute, *supra* note 24, at art. 16; Noone & Moore, *supra* note 39, at 143.

⁹⁹ DoD Law of War Directive, *supra* note 21, at para. 4; U.S. Army and Marine Corps Counterinsurgency Manual, *supra* note 21, at 351-357; JAG Operational Law Handbook, *supra* note 22, at 49-104.

military justice system is swift to act, so complementarity will almost always be present. As the ICC communication concerning Iraq demonstrates, so far the fear of an overzealous prosecutor or trumped-up charges by a political adversary seem to be hyperbolic. There have been nearly eight years of ICC activity, and the ICC has demonstrated restraint and professionalism.¹⁰¹ In contrast, the United States has acted un-statesmanlike with its policy toward the ICC.

Further, the ICC is unlikely to pursue the prosecution of U.S. servicemembers because the ICC needs U.S. support.¹⁰² U.S. obstructionism is currently the single biggest impediment to the development of the ICC.¹⁰³ The ICC cannot have its intended global impact without the support of the world's most influential nation. The United States has always been the main contributor of financial and diplomatic resources as well as subject matter expertise to war crimes tribunals. Without that continued support, the ICC cannot achieve its potential.¹⁰⁴ ICC officials and the international community understand this—they will not carry out a witch hunt against U.S. servicemembers because that would ensure that the United States never gives support to the ICC and certainly never becomes a State Party.

The United States would also benefit from a more cooperative stance toward the ICC by enhancing its reputation internationally.¹⁰⁵ Much of the discussion within the United States about the ICC narrowly focuses on the potential exposure of U.S. servicemembers to ICC prosecution, and more attention should be given to the potential benefits of U.S. cooperation with the ICC.¹⁰⁶

IV. ANY MARGINAL CONSTRAINT ON U.S. ACTION IS OUTWEIGHED BY BENEFITS OF ICC COOPERATION

The need of the ICC for support from the most powerful nation in the world and the need of the United States to enhance its credibility in the world are objectives that can reinforce each other. To the extent that U.S. action is constrained at all by increased cooperation with the ICC, this constraint will be outweighed by increased goodwill amongst the global citizenry, greater legitimacy for U.S. operations abroad, and hence stronger national security at home. Furthermore, from an enlightened self-interest perspective, the ICC

¹⁰⁰ Risch, *supra* note 3, at 77-78.

¹⁰¹ Hatchell, *supra* note 15, at 211; Scheffer, *supra* note 2, at 1575-1579.

¹⁰² Hatchell, *supra* note 15, at 211.

¹⁰³ Scheffer, *supra* note 2, at 1575-1579.

¹⁰⁴ Risch, *supra* note 3, at 80-83, 87; Roth, *supra* note 15, at 57-58.

¹⁰⁵ Scheffer, *supra* note 2, at 1567-1568.

might not be the cure-all for the world's atrocities, but it has the potential to increase stability in the international system.

A. Cooperating with the ICC Will Help Enhance U.S. Global Credibility

For the greatest power on earth to wage its "war on terrorism" by rejecting the very rules of war it is a signatory to, denying justice at home, undermining the U.S. Constitution, and then pressuring its allies to do the same set in motion a devastating denial of civilized instincts. . . . It could well be argued that over time Islamic extremists were emboldened rather than subdued by the travesty of justice the United States perpetrated.¹⁰⁷

Though the above-cited author is not known for dispassionate reporting, his literary works are read around the world and his opinions are shared by a sizeable portion of the global community.¹⁰⁸ This deep-seated belief perseveres for many: the belief that U.S. foreign policy in the years after 9/11 has made the world more unstable.¹⁰⁹ Unfortunately, many believe that the United States does not respect the rule of law.¹¹⁰

The U.S. policy toward the ICC has contributed to this deep-seated belief and has fostered resentment toward the United States that will not dissolve overnight. The United States passed legislation, the ASPA, prohibiting its own agencies from cooperating with the ICC and, further, expended great effort to penalize other nations that chose to cooperate.¹¹¹ The provision in the ASPA that has provoked the greatest hostility toward the United States is the provision giving the President the authority to "use all means necessary and appropriate" to free U.S. servicemembers from The Hague.¹¹² The E.U. Parliament passed a resolution in response to the ASPA, noting that "ASPA goes well beyond the exercise of the United States's sovereign right not to participate in the Court," and that the "bill strongly contrasts with the founding treaties of NATO,"

¹⁰⁶ AHMED RASHID, *DECENT INTO CHAOS: THE U.S. AND THE DISASTER IN PAKISTAN, AFGHANISTAN, AND CENTRAL ASIA* 293-294 (Penguin Books, 2d ed. 2009).

¹⁰⁷ See, Jane Perlez, *Frontier Years Give Might to Ex-Guerilla's Words*, Jul. 5, 2008, THE NEW YORK TIMES, http://www.nytimes.com/2008/07/05/world/asia/05rashid.html?_r=1.

¹⁰⁸ RASHID, *supra* note 105, at Introduction.

¹⁰⁹ See generally RASHID, *supra* note 107; David Mednicoff, *Middle East Dilemmas*, in *PROMOTING THE RULE OF LAW ABROAD: IN SEARCH OF KNOWLEDGE* 252-273 (Thomas Carothers ed., Carnegie Endowment for International Peace 2006).

¹¹⁰ 22 U.S.C. §§ 7401-7432 (2003).

¹¹¹ 22 U.S.C. § 7427 (2003).

dealing a “damaging blow” to U.S. international goodwill.¹¹³ The E.U. Parliament also passed legislation asking E.U. member States to refrain from signing any ASPA bilateral agreements with the United States.¹¹⁴ Members of the Dutch House of Representatives proposed an interpellation expressing their concern over ASPA and noting its harm to “transatlantic relations.”¹¹⁵ Other organizations and many other States have sent letters, held debates, passed legislation, and created websites expressing their resentment toward the United States’ response to the ICC.¹¹⁶

The United States began to mitigate some of this damage once it realized, in the words of former Secretary of State Condoleezza Rice, that cutting off aid to tumultuous countries was “sort of the same as shooting ourselves in the foot.”¹¹⁷ The Obama Administration’s easing of relations toward the ICC helps as well, but ASPA remains in the U.S. Code as a statement of U.S. will, and other nations still regard the United States as hostile to the ICC. The international community believes the United States has back-tracked on its long-standing advocacy for international justice and accountability for atrocities.¹¹⁸ At a time when the United States is trying to regain the moral high ground and instill in other nations a belief that the United States abides by the rule of law, adopting a cooperative stance toward the ICC would be a significant step.

B. Cooperating With the ICC Improves U.S. National Security

Iraq in 2007, and parts of the Afghan campaign in 2006-2008, demonstrated that counterinsurgency can work when done properly. But we must recognize that against the background of an AQ strategy specifically designed to soak up our resources, paralyze our freedom of action and erode our political will through a series of large-scale interventions, counterinsurgency in general is a game we need to avoid wherever possible.¹¹⁹

¹¹² Resolution on the Draft of the American Servicemembers’ Protection Act, EUR. PARL. DOC. PE 319.839 (2002).

¹¹³ Resolution on the International Criminal Court, EUR. PARL. DOC. PE 323.025 (2002).

¹¹⁴ Interpellation Regarding the U.S. American Service Members’ Protection Act, The Netherlands House of Representatives of the States General, 28 437 (June 13, 2002).

¹¹⁵ The American Non-Governmental Organizations Coalition for the International Criminal Court, International Reaction, <http://www.amicc.org/usinfo/reaction.html>.

¹¹⁶ Mark Mazzetti, *U.S. Cuts in Africa Aid Said to Hurt War on Terror*, Jul. 23, 2006, THE NEW YORK TIMES, <http://www.nytimes.com/2006/07/23/world/africa/23terror.html>.

¹¹⁷ Roth, *supra* note 15, at 53-61; Sievert, *supra* note 3, at 98-99.

¹¹⁸ DAVID KILCULLEN, *ACCIDENTAL GUERRILLA: FIGHTING SMALL WARS IN THE MIDST OF A BIG ONE* 267-268 (Oxford University Press 2009).

Direct military interventions are not the solution to the long-term confrontation with international terrorism. Though the United States must maintain its commitments to the people of Afghanistan and Iraq, large-scale military interventions play into the terrorists' exhaustion strategy, create an opening for extremism to seep into the population, and exacerbate global resentment toward the United States.¹²⁰ If the United States is to win the long-term struggle against international terrorism, it must put a new emphasis on the primacy of moral authority, credibility, and partnership building.¹²¹ The current U.S. shortcoming in moral authority and credibility is not solely a result of its position toward the ICC. But the United States' hostile response to the ICC does represent a sizeable portion of the rift between the United States and the rest of the developed world.¹²² It also represents a considerable opportunity for the United States to enhance the cornerstones of its strength: international partnerships and the enlightened pursuit of a stable global society.

Unfortunately, the United States no longer can rely on its military dominance alone to protect its national security.¹²³ In the future, it will be increasingly more difficult for the United States to project military power because of the diffusion of military technology, the continued rise of new military powers, and the problems the United States has had carrying out missions in its vital areas of interest such as the Middle East and Central Asia.¹²⁴ In the early stages of the Iraq and Afghanistan conflicts, the United States assumed that pervasive surveillance, high-technology weaponry, and unlimited cash could quickly accomplish its goals.¹²⁵ The United States is still managing the aftermath of this erroneous assumption. These changes in the global security dynamic cannot be undone, and the United States must adapt.¹²⁶

ICC cooperation represents a U.S. opportunity to reinvigorate existing international partnerships and develop new ones that can strengthen U.S. national security. At both the broad strategic and local tactical level, increased U.S. moral authority and credibility are necessary to garner support. For the foreseeable future, limited U.S. use of military intervention and tactical pursuit of terrorist leaders is necessary.¹²⁷ The United States' adherence to legal standards and the global perception of this adherence will enhance the

¹¹⁹ *Id.* at 184, 268.

¹²⁰ *Id.* at 286; Wheaton, *supra* note 85, at 9-10.

¹²¹ Wheaton, *supra* note 85, at 3-11; Roth, *supra* note 15, at 57-58; Sievert, *supra* note 3, at 98-99.

¹²² KILCULLEN, *supra* note 119, at 264-289; Andrew F. Krepinevich Jr., *The Eroding Foundations of American Power*, 88(4) FOREIGN AFF. 18-33 (2009).

¹²³ Krepinevich, *supra* note 123, at 18-33.

¹²⁴ KILCULLEN, *supra* note 119, at 25, 280-282.

¹²⁵ Krepinevich, *supra* note 123, at 18-33.

¹²⁶ KILCULLEN, *supra* note 119, at 20.

legitimacy of U.S. tactical operations.¹²⁸ More broadly, the United States is losing the information operations aspect of the struggle against extremism.¹²⁹ U.S. cooperation with the ICC would reduce the ammunition available to extremists in carrying out their propaganda bombardment. Establishing the rule of law and good governance is an essential aspect of the current U.S. struggle. Yet, in Arab societies, there exists a “widespread perception that the United States does not in fact practice what it preaches about the rule of law in its own policies.”¹³⁰ Without increased U.S. global credibility, narrow institutional reforms cannot establish the rule of law and a self-sustaining security infrastructure in U.S. vital areas of interest.¹³¹ Moreover, beyond the benefits to the United States, the ICC as an institution has the potential to foster an international environment less hospitable to extremism.

C. The ICC Has the Potential to Improve Global Stability

In formulating its policy toward the ICC, the United States would benefit from a greater appreciation of the purpose of the ICC. The ICC is an attempt to solidify a permanent mechanism for dealing with global atrocities.¹³² Although the war crimes tribunals of the past, including Nuremburg, Rwanda, and the former Yugoslavia, were generally perceived as successful, cobbling together a tribunal after the occurrence of an atrocity is problematic.¹³³ For the United States and the international community, the process of establishing an ad hoc tribunal was extremely costly in time, money, and other resources.¹³⁴ The lack of a permanent system to investigate and prosecute atrocities, coupled with an increase in devastating conflicts, led to near unanimous international support for a permanent institution.¹³⁵

The benefits of a permanent war crimes tribunal are more than economic. Creating a new institution following each atrocity leads to inconsistency and claims of selective justice.¹³⁶ A permanent court has an ongoing presence and operations in addition to institutional knowledge and expertise.¹³⁷ This permanent presence and ongoing operations lead to deterrence and increased global stability, both strongly in the United States’ interests. Accordingly, the United States should not allow the marginal possibility of ICC

¹²⁷ Wheaton, *supra* note 85, at 3.

¹²⁸ KILCULLEN, *supra* note 119, at 58.

¹²⁹ Mednicoff, *supra* note 110, at 252.

¹³⁰ *Id.* at 251-271; KILCULLEN, *supra* note 119, at 264-289.

¹³¹ Scheffer, *supra* note 2, at 1567-1568.

¹³² *Id.* at 1575-1579.

¹³³ Risch, *supra* note 3, at 74.

¹³⁴ *Id.*

¹³⁵ Sievert, *supra* note 3, at 86, 100-110; Noone & Moore, *supra* note 39, at 146.

¹³⁶ Sievert, *supra* note 3, at 86, 100-110; Noone & Moore, *supra* note 39, at 146.

prosecution of U.S. servicemembers to overturn its long history of advocacy and support for war crimes accountability.

The international community cannot and will not revert back to ad hoc international war crimes tribunals.¹³⁷ The ICC is here to stay. If the international community succeeds in this endeavor, if the ICC can accomplish at least a portion of its intended goals, it may prove to be a major development for international justice and global stability. Does it make sense for the United States to resist this development? Just as the United States was at the forefront in developing other major war crimes tribunals—in monetary contributions, expertise and information sharing, and apprehension of fugitives—the United States should position itself at the forefront of the development of the ICC. There is too much at stake to turn away from this opportunity.

V. CONCLUSION

If the United States takes substantive steps toward systematic cooperation with the ICC, it will allow the institution to develop and prove its competency. This will also allow the United States an opportunity to observe the functioning of the ICC and remedy any legal gaps to ensure complementarity.¹³⁸ Up until now the ICC has functioned professionally, and its officials have exercised sound judgment.¹³⁹ In terms of complementarity, the U.S. Code already covers most ICC crimes in one way or another.¹⁴⁰ Though legitimate concerns do still exist, the United States has nothing to gain by analyzing these concerns through a paradigm of hostility. If the Obama Administration truly seeks a new beginning in foreign policy, it needs to realize that the United States has an interest in cooperating with the ICC.

Before the United States can embrace ICC cooperation, it needs the support of DoD and a repeal of ASPA. This law is a misnomer. Like many laws that emanate from Washington, the title of ASPA bears little resemblance to its contents. A U.S. framework for ICC cooperation cannot be established while ASPA and other anti-ICC policies persist.¹⁴¹ Moreover, the persistence of these anti-ICC policies makes the mission of DoD more difficult. U.S. national security in the future will be assured by international partnerships, goodwill amongst the global citizenry, and an overall stable global system. ICC cooperation represents an opportunity for the United States to take a substantive step toward a foreign policy more suitable to the current environment.

¹³⁷ Sievert, *supra* note 3, at 82-103.

¹³⁸ See generally Hatchell, *supra* note 15; Greenawalt, *supra* note 61.

¹³⁹ Risch, *supra* note 3, at 77-78.

¹⁴⁰ Sievert, *supra* note 3, at 119-120.

¹⁴¹ ASIL Independent Task Force Report, *supra* note 13, at 33.

WHEN RUF GETS ROUGH IT LOOKS LIKE R2P: COMPARING MICRO-LEVEL RULES FOR USE OF FORCE IN POST-CONFLICT COUNTRIES CHALLENGED BY ETHNIC, TRIBAL, AND CULTURAL VIOLENCE TO MACRO-LEVEL CONCEPTS OF HUMANITARIAN INTERVENTION AND RESPONSIBILITY TO PROTECT

Lieutenant Commander Scotch Perdue¹

INTRODUCTION

A head of state, faced with mounting evidence that another sovereign is either committing or condoning massive atrocities against the human rights (“HR”) of his or her own people, does not currently have an independent or collective responsibility under international law to intervene – but should there be one? Diplomatic efforts and various types of sanctions aimed at constraining such conduct continue to be an option, but if it becomes apparent that nothing short of use of force will suffice, what would be the legal basis for taking such action?

The Secretary-General of the United Nations intends to develop such a legal framework, called responsibility to protect or “R2P,” to protect persons from large scale HR abuses, but much still needs to be developed at an international level to define how, when, and what amount of force may be used to stop HR abuses in a foreign state.² After all, if a state is unwilling or unable

¹ JAGC, USN. Lieutenant Commander Scotch Perdue deployed to Fallujah, Iraq, in 2008 with 1st Marine Expeditionary Force-Forward where he served as an Operational Law and Detainee Operations Advisor to the Multi National Force-West, Staff Judge Advocate Office. Upon return to the United States, he attended the International Law Masters Program at Georgetown University School of Law where he graduated with distinction and earned a National Security Law Certificate. Currently, Lieutenant Commander Perdue serves as Deputy Legal & Oceans Policy Advisor to the Deputy Chief of Naval Operations for Operations, Plans, and Strategy (N3/5) in the Pentagon.

² The Secretary-General, *Report of the Secretary-General on Implementing the Responsibility to Protect*, ¶ 2, delivered to the General Assembly, U.N. Doc. A/63/677 (Jan. 12, 2009) [hereinafter *Implementing*] (“The task ahead is not to reinterpret or renegotiate the conclusions of the [2005] World Summit but to find ways of implementing its decisions in a fully faithful and consistent

to intervene in HR abuses, the country still remains a diplomatic and political entity that must be respected to preserve international peace and security. Military commanders serving in so called “post-conflict” countries sometimes find themselves on the horns of a very similar dilemma when, through a clash of cultures, they face local, host nation (“HN”) officials who are unwilling or unable to stop perceived HR abuse—and may actually be officially sanctioning the abuse. Yet the commanders must maintain relationships with these officials to continue to work collectively toward local peace and security.

Just as R2P would provide international legal authority to intervene and prevent HR abuses with military force, rules for the use of force (“RUF”) generally provide legal authority for military commanders to intervene with force, up to and including deadly force, as a last resort to prevent an unlawful killing or serious bodily harm. However, having such legal authority does not necessarily make it more likely that such authority will be exercised. To the contrary, because a gun doesn’t have to be fired to “influence the debate,” simply having a weapon and the clear authority to use it may actually decrease the likelihood that a round has to be fired to prevent or minimize harm. What then, if anything, can the micro-application of RUF doctrine by troops in conflict teach about the macro-dynamics of states in conflict to clarify and refine R2P doctrine?

Looking at a large problem in a smaller context can help clarify issues at both the macro- and the micro-levels. This article will explore two examples where RUF must resolve extremely delicate cultural issues and will illustrate how having legal authority to use deadly force is a critical component to the effective resolution of HR conflicts—without needing to actually resort to deadly force. By analogy, this article will argue for developing similar precedent at an international level to minimize the need for actual military interventions to prevent and deter human rights abuses.

Part I will detail micro-level issues faced by military troops on the ground in post-conflict countries. These troops must struggle to determine the type and amount of force needed to effectively prevent HR violations, while still respecting and supporting local governments as viable, legitimate entities on which to build the rule of law. Focusing on comparatively rural, sparsely-populated areas in post-conflict states, the article will draw on two scenarios to examine frictional ethnic, tribal, and cultural influences and explain how military commanders can work within existing legal RUF constructs to leverage legitimized threats of deadly force (hard power) as an effective incentive on local leaders who might otherwise refuse to submit to various economic, social,

manner.”).

and political (soft-power) efforts to deter and prevent HR violations. Specifically, the article will explore how a Commanding Officer, even under extreme time pressure, might initiate a confrontation with local leaders over HR violations by using non-lethal, soft power resources, while never letting those leaders lose sight of the fact that the Commanding Officer has the legal authority and the means to use lethal, hard power force to enforce these overtures.

Next, Part II will turn to the ongoing international legal debate over why, when, and how military force may be legitimately used to intervene to stop intra-national conflicts which threaten massive HR violations. By tracing the concept of R2P from its origin in 2001 to its most recent advances, the article will identify at a macro-level how legal authority for another sovereign state to intervene might enhance the effectiveness of non-military means of persuasion to deter and prevent escalating HR atrocities on an international scale. Preserving international relationships between sovereign states and groups of states that view these conflicts through different diplomatic, political, and legal lenses is challenging but possible.

Part III will tie together the analyses of each scale and argue that lessons can be learned at both the tactical and international levels to conceptualize and implement authorities to deter and prevent HR abuses. States which have allowed cultural or ethnic conflicts within their borders to result in massive HR atrocities share some meaningful similarities with small communities which may ascribe to tribal or cultural norms that lead to smaller-scale, but no less troubling, HR abuses. Comparing the tactical-level approach and the international approach makes clear that the international community must come to a consensus to legalize some form of humanitarian intervention to be maximally effective at deterring and stopping HR violations on a global scale.

The article concludes with a brief commentary about the questionable prognosis for real and lasting change. Rural areas will likely continue to foster troubling tribal values and cultural mindsets long after foreign threats of hard power are removed. Similarly, even with international legal authority in place, heads of state must understand that real change to the underlying ethnic and cultural divides will likely take generations to resolve, whether or not guns are pointed, threats are made, or sabers are rattled. The real key to success will be infinite patience, keen cultural awareness, and tremendous self-restraint. Ultimately, the article argues for an extremely gradual transition in both micro and macro contexts from externally-enforced to internally-embraced efforts to preserve progress and prevent backsliding into an environment that permits HR violations.

TACTICAL ILLUSTRATIONS

Imagine a Commanding Officer for a Marine Battalion Combat Team in al Anbar, Iraq. He is responsible for establishing and maintaining peace and security as well as conducting a wide range of nation-building projects within a vast area of responsibility (“AOR”) covering hundreds of square kilometers of Iraqi desert far to the west of Baghdad. This AOR is only sparsely populated with relatively rural and poor people inhabiting remote towns, villages, and a few minor cities.

One of his subordinate officers radios the Battalion Command Operations Center (“COC”) to report that a local sheik just explained that a tribal court decided to stone a woman accused of infidelity to death at dusk in the marketplace of one of the villages within the battalion AOR. The sheik was just letting the Marines know so that they can “find some other place to patrol this evening.” The officer is seeking guidance on what to do because several males from the village “are digging a big hole and gathering rocks in piles.” Imagine further that this same sheik is the most effective local official in any of the towns in the AOR at helping to identify and deter insurgents, and his village is the center of the most rapidly developing area, with schools, clinics and other thriving initiatives.

The current Rules of Engagement (“ROE”) and Rules for Use of Force (“RUF”), which constrain how and when troops may engage civilians with force, allow the use of deadly force to prevent death or serious bodily injury to civilians.³ Although the CO could deploy Marines to the village with weapons locked and loaded, ready to shoot anyone who picks up a stone, he would immediately recognize how hugely destructive that decision would be to all his past efforts to develop a healthy and productive relationship with the village elders and their sheik. Also, intervening into this emotionally-charged situation could be extremely dangerous for the Marines—and many more civilians than

³ The Department of Defense defines ROE as “[d]irectives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered.” JOINT CHIEFS OF STAFF, JOINT PUB. 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 467 (12 Apr. 2001). “Often these directives are specific to the operation. If there are no operation-specific ROE, U.S. forces apply standing rules of engagement (SROE).” U.S. DEP’T OF THE ARMY, FIELD MANUAL 3-24, COUNTERINSURGENCY, at D-2 (Dec. 2006). “ROE/RUF must always be consistent with the inherent right of self defense, but the specifics that determine when and how that right may be exercised may be different for various missions and weapons systems as determined by the responsible commander.” JOINT CHIEFS OF STAFF, JOINT PUB. 3-26, COUNTERTERRORISM, at V-12 (13 Nov. 2009). For the purposes of this article and these hypothetical situations, we will assume that the relevant ROE and related RUF would authorize the use of force, up to and including deadly force, in all situations involving self-defense or the prevention of death or serious bodily injury to Coalition Force service members and Iraqi civilians.

just the woman—even if the Marines merely sought to take the woman into custody for her own protection.⁴ However, the CO cannot have his Marines simply stand by and allow this public stoning to occur in front of them, either. Nor can he allow them to just “patrol elsewhere at dusk,” as the sheik suggested, which would be an act of willful blindness just as morally and ethically repugnant. So what is the right kind and amount of force appropriate to protect the Marines’ safety, prevent this apparent human rights violation, and still de-escalate this situation in such a way as to preserve crucial relationships?

As the same CO is quickly mulling over that problem, he overhears another call coming into the COC from a different unit under his command. A Marine Police Training Team (“PTT”) Officer in Charge (“OIC”), co-located with Iraqi Police (“IP”), has an urgent issue. The IP Station is located in the center of a small but particularly violent city in the AOR that has had a great number of clashes between various religious factions within the population. The city is filled with corrupt local officials and apathetic if not corrupt police. Shallow graves litter the outskirts of town. The CO recently managed to get the last Chief of Police (“COP”) replaced because he was a puppet-thug; the new COP is much more moderate, extremely well-educated, and professionally trained in westernized police work.

The PTT OIC tells the CO that one of his Marines is at a cell door in the local jail and is holding his weapon on an Iraqi police officer whom he unexpectedly caught torturing a prisoner. The Marine was conducting a routine but unannounced inspection of the jail and happened upon the apparent torture session just as the IP was drawing his police service pistol. They are now in a standoff. The IP is yelling at the Marine to “stay out of Iraqi business,” while he continues threatening to execute the bloodied prisoner. The OIC is headed to the scene with a mobile radio and trying to calm the situation, but the COP is screaming in Arabic, IPs are frantically scrambling to the jail, and the OIC has already sent the remainder of his PTT team to provide armed support to his Marine. The OIC’s interpreter says the COP is ranting that “the Americans have no idea what they are dealing with.” It is not clear whether this is a threat

⁴ Detaining a woman carries its own set of consequential issues. Marines in al Anbar Province in Western Iraq, as well as service members throughout different geographic sectors of Iraq, learned to their dismay that by merely taking Iraqi women into custody (whether because the women were believed to be involved in insurgent activities or criminal conduct or were simply witnesses to such conduct), they had potentially “doomed them to death” under a traditional application of tribal law. This interpretation deems any adult woman who spends more than a few hours in the company of men not from her own family to be “violated” and unacceptable back to her family. The family then becomes obligated to kill the woman to preserve family honor. Interview with Patricio Asfura-Heim, Esq., Research Analyst, Center for Naval Analysis, in Alexandria, Va (Mar. 30, 2009). Mr. Asfura-Heim worked with Marines in Western Iraq in 2007, where he conducted an assessment of tribal customary law.

against the PTT Marines or just the COP blowing off steam about the lingering tensions between uneasy and often unlikely allies. Once again, what is the right kind and amount of force appropriate to protect the Marines' safety, prevent this apparent human rights violation, and deescalate this situation in a way to preserve critical relationships?

PART I: INVESTING IN RELATIONS BUYS TIME IN CRISIS

Whenever you advise a ruler in the way of Tao,
Counsel him not to use force to conquer the universe.
For this would only cause resistance.
Thorn bushes spring up wherever the army has passed.
Lean years follow in the wake of a great war.
Just do what needs to be done.
Never take advantage of power.⁵

Before returning to these illustrative examples, it is important to have a conceptual understanding of some of the cultural factors which affect so much of what troops in post-conflict countries face on a daily basis, particularly in the rural areas. While concentrating on Iraq, including Arab and Muslim culture generally, where appropriate this article will cite parallel examples from other countries and cultures for broader application.

Precious little is written on the specifics of how tribal courts and culture influence society in Iraq, in part because so many nuances exist from one region to another and even from one village to another. The tribal and cultural traditions of western Iraq generally come from the Bedouin tribes, which were historically nomadic. The sedentary tribes of southern Iraq had substantively similar tribal law but distinct procedures and terminology.⁶ As an additional hurdle to learning about this subject, what little is written is rarely translated into languages other than Arabic.⁷ This lack of written record about tribal culture and law is troubling, given its importance both to the people of Iraq and to the

⁵ LAO TZU, *TAO TE CHING* 30 (Gia-fu Feng and Jane English trans., 25th Anniversary ed. Vintage Books 1997).

⁶ Frank H. Stewart, *Tribal Law in the Arab World: A Review of the Literature*, 19 INT'L J. MIDDLE E. STUD. 473, 481 (1987).

⁷ Interview with Patricio Asfura-Heim, *supra* note 4. A 1987 review of existing Arabic literature foretold this dearth of information, not just about Iraq, but across the Arab world, when it concluded that, because so many who dealt with and administered tribal law were illiterate, "in a few decades [documented literature and information regarding tribal law] will almost all be gone. Even such documents as survive will only be partially comprehensible, since it will no longer be possible to elucidate them with the aid of informants from the environment in which they were produced." Stewart, *supra* note 6, at 484.

military service members currently sent to operate there. For the majority of citizens, the customary law is the only law that matters.⁸

For military members of a foreign culture, an awareness and understanding of that customary law are absolutely essential to counterinsurgency (“COIN”) operations.⁹ The Army Field Manual on Stability Operations acknowledges the tension between trying to implement security sector reforms (“SSR”) quickly and needing to take the time to understand the culture (including tribal law) of the region where those reforms will take effect:

Regardless of the need to develop a host nation’s security forces quickly, SSR requires considerable tolerance, cultural awareness, and an environment of mutual respect. In particular, actors working closely with host-nation forces must respect the security culture of the host nation. This culture is shaped by history, language, religion, and customs and must be understood. Cultural awareness and sensitivity are necessary to dispel the natural tensions that arise when external actors dictate the terms and conditions of SSR for the host nation. Responsiveness, flexibility, and adaptability to local culture help limit resentment and resistance to reform while generating local solutions to local problems. Local help fosters acceptance and strengthens the confidence of the citizens in reform.¹⁰

⁸ Historically, “[d]uring long centuries of anarchy, the administration of justice was no longer in the hands of the state ... [and] since only a minority of the population lived in the cities, the law that mattered for most people was the customary law.” *Id.* at 473.

⁹ In an interview with the U.S. Institute for Peace, a member of the Embedded Provincial Reconstruction Team located north of Baghdad with the Second Brigade Combat Team of the 82nd Airborne Division stated,

The only recommendation I could make to people who do not know the culture well is to read as much as you possibly can before going to Iraq. That I did. I read everything I could while I was there.

Another really important thing concerns last summer when some of the brigades got these Human Terrain Teams, which was a new idea that somebody in the army [sic] came up with. The Human Terrain Teams were groups of military officers who were specialists, historians, anthropologists who understood Islamic culture. These were people who at the end of the day we started working very closely with, because even though they did not have the diplomatic skills and the development skills we had, they had a lot of the keys to unlock the mysteries of this culture, so that we could be more effective.

Interview by W. Haven North with Anonymous, Deputy Team Leader, Embedded Provincial Reconstruction Team Baghdad 3 (Feb. 14, 2008), http://www.usip.org/files/file/resources/collections/histories/iraq_prt/2.pdf.

¹⁰ U.S. DEP’T OF THE ARMY, FIELD MANUAL 3-07, STABILITY OPERATIONS, at 6-8 (6 Oct. 2008).

The critical point at the tactical level, which can be extrapolated to the operational or strategic levels, is that, even when there is little to read or rely on, military commanders must make every effort to understand the people with whom they are trying to deal; this will make a significant difference in the likelihood of success. Such investments of time spent on research should be coupled with efforts to build relationships in periods of calm so that there will be shared bonds and grounds for mutual, cross-cultural understanding in times of future crisis.

Let us return to the hypothetical situation of the impending public stoning. As a threshold matter, the CO must decide whether he is obligated by law or policy to take action to prevent the stoning. Is this a purely internal matter that he should let the Iraqis handle on their own, or does international law mandate his intervention? This is an extremely culturally sensitive issue.

From a Western perspective, both the method and alleged justification of such an execution would widely be considered excessive if not baseless punishment that warrants intervention as an HR violation. But in some traditional Arab cultures, an “honor killing” or “honor crime” is the “murder of a girl or woman by her family members due to their disapproval of her alleged sexual misbehavior, which they perceive as defying societal gender norms.”¹¹ These kinds of executions tend to take place in rural areas where a woman can be killed in various ways “in the name of honor when she does something or is thought to have done something that falls outside of her traditional social role.”¹²

Honor killings are relatively rare in the cities and urban areas, and central governments may be slow to enforce change in outlying tribal areas too quickly. Numerous Middle Eastern countries, including Egypt, Jordan, and Kuwait, have drafted laws and adopted constitutions with relatively vague, aspirational language to “recognize established customs as long as they do not conflict with public order or morality.”¹³ Similarly, Article 45 of Iraq’s Constitution says it shall “prohibit the tribal traditions that are in contradiction

¹¹ Rebecca E. Boon, Note, *They Killed Her for Going Out with Boys: Honor Killings in Turkey in Light of Turkey's Accession to the European Union and Lessons for Iraq*, 35 HOFSTRA L. REV. 815, 816 (2006) (citing Dicle Kogacioglu, *The Tradition Effect: Framing Honor Crimes in Turkey*, 15 DIFFERENCES 118, 118 (2004)).

¹² *Id.*

¹³ Mohamed Y. Mattar, *Unresolved Questions in the Bill of Rights of the New Iraqi Constitution: How Will the Clash Between "Human Rights" And "Islamic Law" Be Reconciled In Future Legislative Enactments and Judicial Interpretations?*, 30 FORDHAM INT’L L.J. 126, 139 n.90 (2006). See, e.g., CONSTITUTION OF THE ARAB REPUBLIC OF EGYPT 1400 [1980] art. 12; CONSTITUTION OF THE HASHEMITE KINGDOM OF JORDAN 1952 art. 14; CONSTITUTION OF THE KINGDOM OF BAHRAIN 2002 art. 22; CONSTITUTION OF THE STATE OF KUWAIT 1963 art. 35.

with human rights,”¹⁴ yet Iraq has not taken the “necessary measures, including legislative measures and educational initiatives, to abolish harmful customary practices, such as honor killings.”¹⁵ Thus, even though the written law is gradually moving away from these kinds of HR violations at a national level, at this time, no definitive or pervasive support for eradicating these practices exists within the central Government of Iraq, much less in the rural villages where these violations are still apparently sanctioned.

The lack of central legislative guidance does not mean that forcibly preventing the stoning would not be a “just cause,” but it does mean that, because the sheik will likely be disinclined or unable to stop the killing on his own, some type of force may be necessary to prevent the murder. The CO’s RUF would grant him legal authority to use force, up to and including deadly force, to prevent the woman’s death if he decides that action is appropriate. Recognizing the strong feelings on both sides of this situation, the CO would know that he must approach this delicate issue with something other than brute force, at least initially, or else face an inevitable setback in his ability to form and maintain trusting relationships and make progress in this and other areas.

The first order should be to try to buy time. He should talk to the sheik directly and as soon as possible, and also with the tribal elders who are part of the Sharia court. If the subordinate officer can convince the sheik to hold the status quo until the CO can arrive or if some other meeting place and time can be set up, at least this freezes the crisis.

The next step is to convey a clear and unambiguous message about “intention.” To his own troops, and to the people within the community, the CO can say with sincere conviction that all efforts to prevent the stoning with any means or amount of force will be conducted out of a legitimate intention to protect a life and will be specifically designed to not destroy a way of life. That express goal will likely be of small comfort to the Iraqi people, who will undoubtedly be affected by any show of force that precludes their ability to follow their customs and restore their family’s “honor.” The CO should, as much as possible, work behind the scenes with the sheik and the tribal elders to convince them to take the lead in delaying the stoning and eventually rescinding the decision. If a change is peaceably negotiated, these Iraqi leaders will not want to look like they simply gave in to outside pressure. Thus, the CO will want these leaders to see his face and understand his level of commitment, but then both sides will likely want any changes conveyed to the community by an Iraqi “public face.”

¹⁴ CONSTITUTION OF THE REPUBLIC OF IRAQ art. 45, Second [2005].

¹⁵ Mattar, *supra* note 13, at 139 (footnotes omitted) (arguing that Iraq’s Constitution calls for the abolition of harmful customary practices).

In his meeting with the sheik and elders, the CO can remind them that their own government does not condone the practice of honor killings, and that to carry out such a killing violates formal law. So the CO would have the authority to arrest and prosecute anyone who ordered, participated in, or otherwise facilitated such a killing. He could point to the exceptional progress they have made together as a community to build infrastructure through public works projects. Those projects would necessarily lose funding if the local leaders sanctioned the killing. He could bring in media coverage assets and explain that the sheik and elders may be able to justify their practice in the shadows of a remote village but the world is evolving in a way that rejects these practices. The public at large, beyond the confines of the town, will condemn the leaders for their actions and call into question their own wisdom, justness, and honor.¹⁶ The key message should be that the killing would come at a great cost, jeopardizing all of the progress the CO and sheik have made for the community.

On an even more personal level, in a culture which places extremely high value on respect and honor, the CO could try to use any capital his rank and stature may have to generate buy-in from the “aggrieved” family by saying he wants to meet personally with the head of the family involved to find an amenable alternative solution. This option, depending on circumstances, may be a part of the best solution because it goes directly to the heart of the conflict and will hopefully generate a way to diffuse the tension at a basic level. The list of soft power options is limited only by the imagination, but the CO must make it clear that whether or not the sheik and tribal elders, or the head of household, accept these options as preferable to the stoning, he will use all necessary force to prevent the stoning, so they must find an alternative way to restore honor, through money or some other means.

If these negotiations fail and soft power alone cannot deter the officials or the family, then physical force as a last resort may be unavoidable. The CO’s tacit threat must become a promise or his credibility will suffer irreparable harm. Ultimately, the CO cannot realistically prevent this kind of killing forever—where there is a will, the Iraqis will find a way—but he can realistically prevent this murder from occurring in this market on this evening by cordoning off the square and taking additional measures necessary to disperse any crowds that form. Ideally, he can do this without armed confrontation, and may even be able

¹⁶ Of note, in 2002 and 2003, two Nigerian Sharia courts eventually succumbed to international public pressure to rescind orders to stone two women. See *Nigerian Woman Condemned to Death by Stoning Is Acquitted*, N.Y. TIMES, Mar. 26, 2002, at A5 (describing the verdict for Ms. Safiya Hussaini); Editorial, *Saved from Stoning*, N.Y. TIMES, Sept. 27, 2003, at A14 (speculating on potential motivations behind the reversal of Ms. Amina Lawal’s conviction).

to find safe haven for the intended female victim if they can identify her. The CO must draw the line and then enforce it through a thoughtful, culturally sensitive series of negotiating points and escalating pressures to dissuade the HR violation. Self-restraint is critical, and the CO should, as visibly as possible, show that he is seeking a balance of proportional means to prevent the abuse while preserving relationships where possible.

Taking life to save life is philosophically problematic. Even on a purely practical level, if the Marines fire at anyone in the crowd and wound or kill people as a “deterrent” or “preventive measure” to stop a perceived HR violation, their legitimacy would be undermined, not strengthened. Such an act would likely be perceived as unjustly executing the judges, jury, and citizens of the gallery in place of the condemned criminal, effectively turning the whole matter into an unwinnable clash of religious, cultural, and ethnic wills, where neither side can honorably submit or retreat. Alternatively, if Marines proceed methodically through as gradual an escalation of force as possible, then legitimacy will have the best chance of surviving. If the Marines start with non-lethal efforts to warn and disperse the crowd—or if they take the woman into protective custody—and resort to deadly force only when absolutely necessary to prevent the HR violation or defend themselves, the Marines may still be criticized by the community, but their reputation as credible brokers will be maintained.

The next concern for the CO is determining which courses of action offer the most reasonable prospects for success. This decision turns almost wholly on the definition of “success” in this context. The Marines would certainly have sufficient firepower to completely and effectively prevent this specific stoning, but if the Marines are only able to prevent the stoning by killing others, or future honor killings continue to occur (but in secret), then the Marines would have succeeded in “winning the battle and losing the war,” all at once. The CO is likely to approach this entire matter with the understanding that there really are no unambiguous winners in these humanitarian intervention scenarios where success is a necessarily relative term.

The truer measure of success would be the degree of permanency in changing minds about the legitimacy of this and all future honor killings. Such a long-term view of this short-term crisis is critical to an adequate analysis of what type and amount of force will be appropriate for ensuring “success,” whether or not hearts and minds are truly won. Stopping the violence is only the beginning. Once the immediate crisis is either averted or quelled for the time being, the CO must implement education programs, public outreach and women’s engagement efforts, and other soft-power measures to try to seek alternative resolutions and head off similar confrontations in the future. His

message must be one that acknowledges the importance of custom, while forcefully encouraging at least gradual evolution toward an acceptable common ground to preserve the ability to move forward in this and all other developmental areas.

Finally, throughout this action plan, regardless of which paths it may take, the CO must never allow the sheik or the tribal elders to lose sight of the fact that he has legitimate authority to intervene with any means necessary to protect life. The importance of the underlying legal footing for service members which derives from the ROE and RUF cannot be overemphasized. Both the military CO and his troops, as well as the local public officials and tribal elders, must have no doubt that the military will approach this matter with a firm conviction that the ROE and RUF make it legal to use force, “up to and including deadly force to prevent death or serious bodily injury.”¹⁷ The legal support provides the backbone to any threat to use military force, leaving no question that the military will act with deadly force if it must. The legal backing puts the military commander in a maximally powerful position, because his threats in this regard, whether explicit or implied, are credible. If the legal backing were ambiguous, then the local officials would have some measure of leverage against the CO or his superiors, and the military might hesitate to use deadly force to prevent the HR abuse. This manifest pressure can also be manipulated in a variety of ways to try to make this bitter pill as palatable as possible to those who must swallow it. If everyone knows the Marines have the legal authority and the will to use deadly force, it empowers the sheik and tribal leaders to put whatever public face on the message they wish.¹⁸

An effort by the CO to remain in the background, if possible, keeps the palpable threat of force in the public consciousness, but avoids a direct clash of wills. The people may accept the political spin and be pacified by the soft power options, or they may continue to interpret this as an unacceptable affront and force the issue. If that occurs, the CO may want to try to again maneuver U.S. troops out of the direct path of anger and deflect it somewhat with a multilateral approach involving Iraqi Police or other security forces to essentially enforce the law as directed by the central government of Iraq.¹⁹

¹⁷ See *supra* note 3.

¹⁸ The public officials and local leaders might explain how they fought on behalf of the tribal heritage and won several concessions from the negotiations, how the critical matter of community honor will be resolved in due course in a way that will not jeopardize more lives, and how, in the meantime, the community will benefit from new social and financial opportunities.

¹⁹ The message in this instance would be, “This is not an ‘America versus Iraq’ issue, or a ‘Christian versus Muslim’ issue; this is a ‘tribal past versus international future’ issue that your own government is imposing.”

This may be a tough sell to the Chief of Police, who likely will not want to get roped into a political imbroglio, but this is precisely the kind of civil matter that he and his police officers must be trained to deal with. Their shared nationality with the villagers adds an intangible dynamic to the debate over legitimacy and is a critical consideration for the long-term enforceability of these kinds of restrictions on HR violations. In reality, such a complex and tense situation may give rise to legitimate concerns about the understandably mixed loyalties of police officers, and the resulting ability to effectively control IP assets. Ultimately, this is a matter of training rather than policy. A preference for incorporating host-nation law enforcement assets into resolving what is essentially an internal matter of great ethnic, tribal, and cultural significance also characterizes the tensions inherent in the HR violation scenario involving police threatening a prisoner with execution.

Building the kind of professional rapport necessary to work effectively with host-nation police would be difficult if the military personnel who are assigned to train and work with the police on a protracted daily basis occasionally threaten to kill them if they don't get it right. Not to make light of this troubling dynamic, this scenario captures the exquisite tension that exists between deeply ingrained cultural perspectives that conflict directly on a major point of contention.

In its 2007 Handbook on Security System Reform, the Development Assistance Committee ("DAC") of the Organisation for Economic Cooperation and Development ("OECD") asserted that, "[s]uccessful police reform requires widespread acceptance of change across ranks and units, but some officers will not modify their behaviour unless they believe it is in their personal interest."²⁰ The Handbook lists promotions, pay increases, and other economic incentives as carrots to offer in this regard,²¹ but these carrots will not change the mindset of an individual police officer who, like most IP, is likely to have an ingrained perspective that police are unofficially authorized to use brutality and even conduct extrajudicial killings where "necessary" in seeking "justice." Often these conflicted perspectives are further fueled by racial or ethnic tensions that revolve around concepts of varying degrees of value for human life based on competing religious, ethnic, or tribal affiliations (*i.e.*, "He is not of my people and therefore little better than a dog. He deserves what he gets."). This is the underlying social reality facing the CO as he starts to analyze competing courses of action for dealing with the second scenario.

²⁰ DEV. ASSISTANCE COMM., ORG. FOR ECON. CO-OPERATION & DEV., THE OECD DAC HANDBOOK ON SECURITY SYSTEM REFORM: SUPPORTING SECURITY AND JUSTICE 170 (2007).

²¹ *Id.*

Again, the military CO must start with the threshold question of whether intervention into a particular matter is within the scope of his mission. If so, he must answer what type and amount of force is best suited to resolve the matter, protect his troops, and, to the greatest extent possible, preserve existing relationships for the future. From a Western perspective, preventing the torture and murder of prisoners is a core part of the police training and reform mission tasked to the CO, so intervention in this situation is appropriate and necessary.

But quickly convincing a group of IPs that the life of an alleged criminal is worth the same as a police officer's life is simply unrealistic, particularly if the prisoner is from a rival ethnic or religious group. Similarly, the concept of rightful intention is likely to generate divisiveness when IPs may superficially accept the notion that all human life is valuable but they are unable to apply that concept to a specific context. After all, they may see their draconian methods of gathering "confessions" and dealing with criminals as a necessary deviation from an idyllic approach that values all life. The IP may see their approach as justifiable, particularly if the American counterargument ironically threatens deadly force to enforce a view that values all life.

Using deadly force is again a last resort. The CO needs to buy time. Hopefully, he still has the time and means to leverage the Chief of Police to calm the situation without bloodshed. This scenario mixes both self-defense and HR intervention in such a way that use of deadly force may result from an unfortunate inability to communicate effectively in a timely manner to avert the crisis. The CO, if he thinks it is appropriate, can make the unorthodox order to temporarily restrict the use of deadly force to only cover self-defense and not the protection of the prisoner. He can tell the COP, "My Marine will not shoot unless personally threatened. You need to have your people calm down, and we will meet to discuss this immediately." Neither side sincerely wants to kill the other, so lowering weapons and letting cooler heads prevail is a strong argument.

In determining the appropriate proportional force to employ, the CO faces a challenge as difficult as the first scenario posed. Iraqi-on-Iraqi abuse and the murder of state prisoners (termed "extrajudicial killings") has, at times, been absolutely systemic in Iraq.²² Troops on the ground face the challenge of responding to individual abuse, as well as systemic policies of abuse. Even so, the self-defense aspects of this scenario will define the scope of the response. Defining success or failure in this context is complex. The stand-off and

²² BUREAU OF DEMOCRACY, HUMAN RIGHTS, & LABOR, DEP'T OF STATE, 2009 COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES: IRAQ (Mar. 11, 2010), *available at* <http://www.state.gov/g/drl/rls/hrrpt/2009/nea/136069.htm> (noting that unauthorized government agent involvement in extrajudicial killings was widespread and confirmed in years past but largely ceased in 2009).

credible threat of deadly force may already have caused irreparable harm to the ongoing ability to work professionally together. Rebuilding trust in the future will be difficult, but at least the Americans will have shown an extreme level of commitment to the ideals they are trying to instill in local law enforcement. An unwavering commitment to human rights, coupled with a show of self-restraint by the Americans in trying to resolve the matter, will broadcast a clear set of expectations to the IP and cement their understanding of conduct Americans will not tolerate.

Ideally, once this kind of stand-off occurs, the lessons learned from the incident will serve as a strong disincentive for IPs considering similar actions in the future. Knowledge that the Americans can, and will, use lawful deadly force to prevent HR violations will be a significant influence on future behavior. As before, changing hearts and minds in this environment will be gradual, so maintaining strong relationships based on ever-increasing mutual understanding—and hopefully mutual respect—will be critical.

Both of these scenarios show (1) that legitimacy and credibility can stem from legal authority, (2) that cultural awareness can enhance creativity in crisis resolution, and (3) that constant pressure applied in a self-restrained manner can preserve relationships as a foundation for future progress. These principles can be similarly employed to deter international HR violations.

PART II: DEFINING THE BOUNDS OF LEGAL AUTHORITY BEYOND SELF-DEFENSE

“Power is no Blessing in itself But when it is employed to protect the Innocent . . . , then it becomes a great Blessing.”²³

The Charter of the United Nations (“U.N.”) reads, “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations;”²⁴ however, nothing in the U.N. Charter “shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain inter-national peace and security.”²⁵

²³ Jonathan Swift, *On Mutual Subjection*, in *THREE SERMONS* 1, 18 (London, R. Dodsley 1744).

²⁴ U.N. Charter art. 2, para. 4.

²⁵ U.N. Charter art. 51.

In light of the premise that one of the primary, driving purposes of the U.N. was to “save succeeding generations from the scourge of war,”²⁶ these two provisions of the Charter, taken together, maintain that states should refrain from the use of military force unless such force is absolutely necessary to respond in self-defense to an actual attack by another state. Even then, under the requirement for proportionality, the defending state should only use the force absolutely necessary to defend itself (individually or collectively) until the U.N. Security Council can act to otherwise restore peace and security. This is the narrowest reading of states’ rights and obligations for use of military force under the U.N. Charter, and its actual protection understandably begins to feel as thin as the paper it is printed on when held up against the looming threats to peace and stability which exist in the world today.

Whether considering types of threats (*e.g.*, nuclear weapons and other weapons of mass destruction) or sources of such threats (*e.g.*, rogue states, terrorist cells, or other non-state actors), there can be an understandable, natural anxiety about the adequacy of protection offered by an idealistic international legal policy which attempts to severely constrain the ability of states to unilaterally use military force in self-defense until after irreparable harm is already likely to be suffered.²⁷ Related concepts and concerns regularly surface in debates over the internationally acceptable limits of preemptive and

²⁶ U.N. Charter pmb1. This article sets aside any debate about the past, current, or future validity of the U.N., its Security Council, or any other specific U.N. organ, regarding its ability to affect or control individual state behavior. See generally John Norton Moore, *Toward a New Paradigm: Enhanced Effectiveness in United Nations Peacekeeping, Collective Security, and War Avoidance*, 37 VA. J. INT’L L. 811 (1997) (describing the historically episodic success of U.N. peacekeeping and suggesting ways to make the U.N. more credible and effective at deterring war). For the sake of argument, I presume that the U.N. plays an influential role in defining the legal authority for individual states to exert military force against other sovereign states within the international community. The specific focus here will be on the ongoing debate regarding whether and when states, individually or collectively, can legitimately use military force to intervene in a perceived humanitarian crisis somewhere in the world.

²⁷ The concept of preventive self-defense as applied to international use of force was most famously articulated by President George W. Bush in his commencement address at West Point in 2002 and by his incorporation of the “Bush Doctrine” into the National Security Strategy that year. See Commencement Address at the United States Military Academy in West Point, New York, 1 PUB. PAPERS 917, 919 (June 1, 2002) (“We must take the battle to the enemy, disrupt his plans, and confront the worst threats before they emerge.”); THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 14 (2002), available at <http://georgewbush-whitehouse.archives.gov/nsc/nss/2002/nss.pdf> (“We must be prepared to stop rogue states and their terrorist clients before they are able to threaten or use weapons of mass destruction against the United States and our allies and friends.”). But other controversial “anticipatory” uses of military force, such as the widely condemned 1981 bombing of the Iranian Osirak Reactor by Israel, illustrates the same line of thought. See S.C. Res. 487, ¶ 1, U.N. Doc. S/RES/487 (June 19, 1981).

anticipatory self-defense, as well as in the context of humanitarian intervention.²⁸

This article will not recount in any particular detail the horrors and atrocities of national-level human rights violations in places like Bosnia, Rwanda, or Darfur that are already well-documented in the media, professional literature, and records of international courts and tribunals.²⁹ These human rights violations have sparked and fueled the international debate about whether humanitarian intervention is an appropriate context to legitimize and legalize the use of force.³⁰ Suffice it to say that in each of these examples, the level of violence was extreme. Whether in the form of rampant murder in thinly veiled attempts at ethnic cleansing, wholesale slaughter on a genocidal scale, or systematic rape and other forms of intimidating brutality, the populations of these countries suffered tremendous loss of life and collective mental trauma before any international decisions to intervene militarily could come to fruition.

²⁸ See generally, e.g., Niaz A. Shah, *Self-Defence, Anticipatory Self-Defence and Pre-Emption: International Law's Response to Terrorism*, 12 J. CONFLICT & SECURITY L. 95 (2007) (arguing that the doctrine of pre-emption cannot fit into the current international legal system); George A. Critchlow, *Stopping Genocide Through International Agreement When the Security Council Fails to Act*, 40 GEO. J. INT'L L. 311 (2009) (advocating support for an international treaty that sets forth standards and criteria for humanitarian intervention to prevent genocide).

²⁹ In Rwanda, organized Hutu militias killed some 800,000 Tutsis and moderate Hutus in an unprecedentedly fast genocidal spree, beginning in April 1994. U.S. DEP'T OF STATE, BACKGROUND NOTE: RWANDA (2009), <http://www.state.gov/r/pa/ei/bgn/2861.htm>. In Bosnia, the Army of Republika Srpska (Bosnian Serb Army) killed more than 8,000 Bosnian Muslim men and boys during the Srebrenica Massacre in July 1995. U.S. DEP'T OF STATE, BACKGROUND NOTE: BOSNIA & HERZEGOVINA (2009), <http://www.state.gov/r/pa/ei/bgn/2868.htm>. Hundreds of thousands of civilians have been killed by the Janjaweed militias in Darfur. BUREAU OF DEMOCRACY, HUMAN RIGHTS, & LABOR, DEP'T OF STATE, 2009 COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES: SUDAN (Mar. 11, 2010), available at <http://www.state.gov/g/drl/rls/hrrpt/2009/af/135978.htm> (citing U.N. estimates that, as of 2008, up to 300,000 persons may have been killed as a result of the conflict and nearly 3 million civilians had been displaced since 2003). For examples of scholastic reviews of these atrocities and their legal implications, see generally, Gregory L. Naarden, *Nonprosecutorial Sanctions for Grave Violations of International Humanitarian Law: Wartime Conduct of Bosnia Police Officials*, 97 AM. J. INT'L L. 342, 342-52 (2003) (suggesting nonprosecutorial mechanisms to assign accountability for human rights atrocities); Okeckukwu Oko, *The Challenges of International Criminal Prosecutions in Africa*, 31 FORDHAM INT'L L.J. 343 (2008) (assessing as insurmountable the difficulties of international criminal prosecutions in Africa); John E. Tanagho & John P. Hermina, *The International Community Responds to Darfur: ICC Prosecution Renews Hope for International Justice*, 6 LOY. U. CHI. INT'L L. REV. 367 (2009) (examining the international response to Darfur and calling for international affirmation of R2P as international law). Records and court documents from international tribunals are readily available on the Internet. See generally, e.g., <http://www.icc-cpi.int/Menus/ICC/Situations+and+Cases> (International Criminal Court); <http://www.unict.org> (International Criminal Tribunal for Rwanda); and <http://www.icty.org> (International Criminal Tribunal for the former Yugoslavia).

³⁰ See, e.g., Press Release, General Assembly, Delegates Weigh Legal Merits of Responsibility to Protect Concept as General Assembly Concludes Debate; Speakers Question its Effectiveness in Face of Security Council Veto Power, U.N. Doc. GA/10850 (July 28, 2009).

The hard question, simply put, was and is, “How many must be allowed to die before others can stop the killing?” Of course, the complexity of the issues involved rapidly expands the series of questions that must be asked and answered such as: Does the nature of the violence warrant international intervention? What non-military measures are available to try to end the violence? How long should the nations of the world attempt to rely on economic, political, diplomatic, and other non-military measures before resorting to military intervention as a last resort? Or, if we collectively agree that we have reached the unfortunate point where military intervention is the only realistic means available to end the violence, which countries will intervene with force, with how many troops, with what kinds of weapons, and for how long? This last question is the proverbial “million dollar question” (or more literally, the “billions of dollars question”) which comes with no guarantees that even a broad-based and well-trained force of disciplined international troops can effectively intervene, swiftly end bloodshed, and deftly extricate itself from the aftermath. To the contrary, experience shows that there are many devils in the details of these operations, and the international debates reflect that reality.

The International Commission on Intervention and State Sovereignty (“ICISS”) espouses a forward-leaning position that sovereign states, beyond having a “right” to intervene if things get bad enough in another state, actually have an international responsibility to first protect the people of their own state, and then a secondary, yet related, responsibility to effectively protect all people of all states on a global scale.³¹ This social theory of responsibility to protect, or “R2P,” is an emerging conceptual framework on an international scale for trying to deal with humanitarian intervention scenarios, but it needs clarification as to actual implementation.³²

³¹ INTERNATIONAL COMMISSION ON INTERVENTION AND STATE SOVEREIGNTY, THE RESPONSIBILITY TO PROTECT 17 (2001) [hereinafter ICISS].

³² See Siobhán Wills, *Military Interventions on Behalf of Vulnerable Populations: The Legal Responsibilities of States and International Organizations Engaged in Peace Support Operations*, 9 J. CONFLICT & SECURITY L. 387, 387-88 (2004), in which the author states:

[T]he international community has a responsibility to ensure that the basic human rights of peoples are respected everywhere. Where a state fails to ensure the protection of its citizens from serious violations of those rights, it may be legitimate to undertake military intervention (but only if no less intrusive method of ensuring protection is likely to be effective). However the extent to which the intervening state or organisation has a responsibility to ensure protection of those rights *after* it has intervened is not so clearly articulated.

See also Press Release, General Assembly, General Assembly Adopts Resolution Stressing Critical Need for Regional Approach to Conflict Prevention in Africa; Implementation of Responsibility to Protect: Secretary-General's Three-pillar Approach is Focus of Subsequent Debate, U.N. Doc. GA/10848 (July 28, 2009), in which Assembly President Miguel d'Escoto Brockmann noted that many Member States hesitated to embrace the doctrine [of R2P] and its aspirations, not out of indifference to the plight of many who suffered at the hands of their own Governments, but due to a fear that the current system of collective security had not evolved to the degree that would allow the doctrine to operate in the intended manner.

The noted humanitarian law scholar and author Dr. Siobhán Wills wrote that there should be a “shared responsibility” between individual states and the international community “to prevent and punish serious violations of human rights . . . if the state is either unwilling to meet its international obligations or, in the case of ‘weak’ or ‘failed’ states, unable to prevent serious violations from being committed on its territory by private parties.”³³ Citing to basic principles outlined by the ICISS, Dr. Wills clarifies that states normally remain in a default self-restraint mode against external intervention. But when “a population is suffering serious harm, as a result of internal war, insurgency, repression or state failure, and the state in question is unwilling or unable to halt or avert it, the principle of non-intervention yields to the international responsibility to protect.”³⁴

On the opposite side of the debate, critics of the R2P concept argue that the U.N. Charter does not, and should not, provide a legal basis for military intervention to stop human rights abuses.³⁵ These critics argue that humanitarian intervention is an excuse for powerful states to initially violate state sovereignty and impose democracy.³⁶ From a moral perspective, R2P critics object to a line of reasoning that finds legal validity in taking life to save life, particularly on such a large scale.³⁷

In response to these kinds of criticisms, scholars and diplomats have discussed, over the past decade in particular, the scope and parameters within which a humanitarian intervention might be legitimate. An early work from 2001, focusing on the conflict in Kosovo, listed six possible interrelated factors to frame a decision to intervene for humanitarian reasons: (1) sufficiently credible evidence of actual human rights violations, (2) adequate indication that

³³ Siobhán Wills, *supra* note 32, at 388.

³⁴ *Id.* at 389 (citing ICISS, *supra* note 31, at XI).

³⁵ The President of the General Assembly, *Concept Note on the Responsibility to Protect Populations from Genocide, War crimes, Ethnic Cleansing and Crimes Against Humanity*, at Annex, delivered to the General Assembly, U.N. Doc. A/63/958 (Sept. 9, 2009) (arguing against R2P from a national-sovereignty standpoint).

³⁶ General Assembly President Miguel D'Escoto Brockmann of Nicaragua was outspoken in opposition to a legal mandate for R2P. *Id.*; see also General Assembly President, Statement at the Opening of the Thematic Dialogue of the General Assembly on the Responsibility to Protect (July 23, 2009) (transcript available at <http://www.un.org/ga/president/63/statements/openingr2p230709.shtml>) (“[T]here is little reason to doubt that endorsement of R2P by the General Assembly will generate new ‘coalitions of the willing’, crusades such as the intervention in Iraq led by self-appointed saviours who arrogated to themselves the right to intervene with impunity in the name of overcoming nation-state impunity.”).

³⁷ This precise moral conundrum, though on somewhat different scales, is implicated in the localized hypothetical examples presented at the beginning of this Note.

these violations are of sufficient scale to warrant intervention, (3) exhaustion of all reasonable non-military means to stop the violations, (4) some indication that the victims of the abuse are seeking outside intervention, (5) an agreed upon limit to the scope of the military intervention (*i.e.*, size and duration), and (6) multilateral agreement on the objectives of the intervention.³⁸ Six years later, Professor Christopher C. Joyner, citing the scholarly research of Rudolph Rummel on armed conflict in the twentieth century, argued that “innocent people killed by their own governments are of such a magnitude that it is difficult to relate to or appreciate their meaning.”³⁹ During the twentieth century, interstate wars took the lives of thirty-five million military members, but internal conflicts resulted in 170 million civilian casualties—nearly five times the number—often at the hands of their own governments’ agents.⁴⁰ After recounting horrific atrocities suffered in Bosnia-Herzegovina and citing the numbers of civilian deaths in Nigeria, Indonesia, Uganda, and Cambodia as indicative of the depth of depravity of some totalitarian rulers such as Idi Amin or Pol Pot, he argues, “Surely international law cannot condone under any circumstances such massive butchery of a people by its government.”⁴¹ As an answer, Professor Joyner concludes, similar to Professor Wills, that the international community must rethink the concept of sovereignty and adopt a responsibility to protect. This responsibility begins with and is “motivated by the supreme duty of a government to protect its population, without a legal license to kill massive numbers of that population.”⁴²

Central to this argument is the idea that the legal underpinnings of a new responsibility to protect through humanitarian intervention must actually be kept conceptually distinct from a traditional self-defense analysis. Self-defense covers “actions [which] states are permitted to take when confronted with real or perceived attacks on their territory or against their own nationals, as authorized by the principle of self-defense as set out in Article 51 of the UN Charter or through the authority of the Security Council.”⁴³ Professor Joyner argues that, “[u]se of ‘responsibility to protect,’ instead of the more proverbial ‘right to intervene,’ furnishes greater worth to the humanitarian issues in question. It adds a positive, more humane context to what is clearly a terrifying situation inside a state.”⁴⁴ This leads ultimately to his conclusion that, “[t]he notion of sovereignty should be [re]conceived as the preeminent need for the government

³⁸ John J. Merriam, Note, *Kosovo and the Humanitarian Intervention*, 33 CASE W. RESERVE J. INT’L L. 111, 126-36 (2001).

³⁹ Christopher C. Joyner, “*The Responsibility to Protect*”: *Humanitarian Concern and the Lawfulness of Armed Intervention*, 47 VA. J. INT’L L. 693, 694 (2007).

⁴⁰ *Id.* (citing R. J. Rummel, DEATH BY GOVERNMENT 9-12 (1994)).

⁴¹ *Id.* at 696.

⁴² *Id.*

⁴³ *Id.* at 700.

⁴⁴ Joyner, *supra* note 39, at 708.

of a state to exercise responsibility, not merely control over its actions.”⁴⁵ A government’s paramount duty is to “protect its population without any alleged legal license to kill massively selected members within it.”⁴⁶

Thus, from the foundations laid by ICISS and proponents of the “responsibility to intervene,” and incorporating the tragic experience of an additional six years of the world’s struggle to decide how to deal effectively with repeated examples of extreme HR violations, Professor Joyner fleshed out six “thresholds” which states would need to address before responsibly and legally resorting to humanitarian intervention.⁴⁷ The six thresholds track along the same lines as the ICISS criteria and include “just cause,” “rightful intention,” “last resort,” “proportional means,” “reasonable prospects for success,” and “legitimate authority.”⁴⁸

Upon examination of the scenarios laid out in Part I of this article, all of these specific criteria proposed for consideration by heads of state at the international level are incorporated to some extent into the decision-making process of Commanding Officers at the troop level. They are the same kinds of criteria that make COs’ decisions to use force both legal and legitimate. They are also the criteria that make hard-power threats maximally credible, and enhance the persuasiveness of soft-power overtures.

In recognizing a need for legal legitimacy, heads of state and the U.N. General Assembly agreed, “Each individual State has the responsibility to protect its populations from genocide, war crimes, ethnic cleansing and crimes against humanity. This responsibility entails the prevention of such crimes, including their incitement, through appropriate and necessary means. We accept that responsibility and will act in accordance with it.”⁴⁹ In the 2005 World Summit Outcome, the General Assembly stated its collective commitment to use force to protect people when soft power fails to stop large-scale HR abuses:

The international community, through the United Nations, also has the responsibility to use appropriate diplomatic, humanitarian and other peaceful means, in accordance with Chapters VI and VIII of the Charter, to help to protect populations from genocide, war crimes, ethnic cleansing and crimes against humanity. In this context, we are prepared to take collective action, in a timely and decisive manner,

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.* at 712-16.

⁴⁸ Compare *id.* with ICISS, *supra* note 31, at XI.

⁴⁹ 2005 World Summit Outcome, G.A. Res. 60/1, ¶ 138 (Oct. 24, 2005).

through the Security Council, in accordance with the Charter, including Chapter VII, on a case-by-case basis and in cooperation with relevant regional organizations as appropriate, should peaceful means be inadequate and national authorities are manifestly failing to protect their populations from genocide, war crimes, ethnic cleansing and crimes against humanity.⁵⁰

In 2009, the Secretary-General of the United Nations affirmed the 2005 World Summit Outcome as the overarching legal authority for future action:

Based on existing international law, agreed at the highest level and endorsed by both the General Assembly and the Security Council, the provisions of paragraphs 138 and 139 of the [2005 World] Summit Outcome define the authoritative framework within which Member States, regional arrangements and the United Nations system and its partners can seek to give a doctrinal, policy and institutional life to the responsibility to protect (widely referred to as “RtoP” or “R2P” in English).⁵¹

The debate about exactly how to implement R2P is precisely where comparing micro and macro concepts is most useful.

PART III: CONCLUSIONS FROM COMPARISONS OF SCALE

Under the emerging doctrine of R2P, the Secretary-General describes the responsibility to protect as resting on three pillars: (1) “The protection responsibilities of the State,” (2) “International assistance and capacity-building,” and (3) a “Timely and decisive response.”⁵² The military Commanding Officer is trained to understand that everything his or her troops do, or fail to do, is his or her individual professional responsibility. Under the first pillar, heads of state are being held to a comparable standard.⁵³ Allowing for some flexibility based on scale within the analogy, if a country’s leader has a problem that rises to the level of “genocide, war crimes, ethnic cleansing and crimes against humanity,” then he or she is responsible and must take action. If that leader cannot handle the situation internally, then the second pillar treats

⁵⁰ *Id.* at ¶ 139.

⁵¹ *Implementing*, *supra* note 2, at ¶ 2.

⁵² *Id.* at ¶ 11.

⁵³ *See id.* at ¶ 18 (“[T]he obligations of States that underpin pillar one are firmly embedded in pre-existing, treaty-based and customary international law.”).

those four specified circumstances (*i.e.*, genocide, war crimes, ethnic cleansing and crimes against humanity) as the same kind of triggering criteria as “death or serious bodily harm,” which legally authorizes a CO to intervene—with deadly force if necessary.⁵⁴ The third pillar calls for timely and decisive action. Heads of state, just like COs, must find ways to escalate through soft-power options, emphasizing a firm resolve to use hard-power options if necessary, in such a way that they effectively prevent and deter HR violations, but still preserve, to the extent possible, the ability to continue to work together after the crisis to build positive relationships.⁵⁵

Heads of state must acknowledge a tension between a desire for multilateral action (or clear sanction by a multilateral body like the U.N. Security Council) and the priority for timely and decisive action, which necessarily favors unilateral action. Building international consensus and coalitions for intervention inevitably takes more time.⁵⁶ International multilateralism is certainly worth the wait when it tends to enhance legitimacy of any action taken in the long run.

A mandate for decisive action, tempered by a preference for multilateral action, sends the strongest signal that the international community must legalize some form of R2P to legitimize and strengthen all non-military efforts to deter HR violations on two fronts. First, regarding potential allies in an intervention, having clear legal authority streamlines the debate. Second, regarding the state which is unwilling or unable to stop its HR abuses, the international community does not have to resort to military force to significantly influence the thought process of that country’s leaders if it truly believes the “gun” is loaded and ready to fire as a concluding remark.

Along these same lines, heads of state, just like COs, should avoid taking on any intervention with the idea that it will simply be a matter of getting in, dealing with the immediate crisis, and then walking away clean. In both micro and macro contexts, officials must make a concerted effort over time to

⁵⁴ See *id.* at ¶ 40 (“[C]ollective international military assistance may be the surest way to support the State in meeting its obligations relating to the responsibility to protect.”).

⁵⁵ See *id.* at ¶ 51 (“[P]illar three encompasses, in addition to more robust steps, a wide range of non-coercive and non-violent response measures.”).

⁵⁶ The ICISS has noted that the “Operational Dimension” of intervention often comes face-to-face with policy differences between partner nations:

The effort to build broad support for an intervention action often confronts the problem that coalition partners may well have different ideas about the objectives to be achieved through the intervention action. Ideally, the process of making a decision to intervene, the formulation of the mandate for the intervening agent (or combination of agents), and the allocation of structures and means for implementation should be related. But harmonizing the views and interests of differing states in each regard is often a protracted and complex undertaking.

ICISS, *supra* note 31, ¶ 7.14, at 59.

learn about the cultural situation and the reasons for the crisis, to apply that knowledge in formulating meaningful soft power options, and then to follow through (no matter how long it takes) with threats to prevent and deter the HR violation. Failure to remain engaged in combating the HR abuses will severely undermine credibility and weaken the ability to build trust or respect in the future.

The so-called “Pottery Barn Rule” of military intervention stands for the proposition that if “you break it, you own it.”⁵⁷ This is to say, if a country takes military action in a foreign land and damages the local government, the intervening country has the responsibility to restore the state to a functioning society. To this end, the advice of Professor Michael J. Glennon is probably ideal but realistically impossible to follow. He argues that intervening states, specifically the United States, should concentrate on preventing HR abuses, rather than reconstituting nations’ systems of governments:

The United States needs desperately to keep its eye on the ball: the point of intervention is not to build nations, not to re-engineer foreign societies into ‘better’ ones formed in the image and likeness of a multicultural America - if that is indeed where the United States is or wishes to go. *The point of intervention is to halt mass murder, nothing more and nothing less.* The point is *not* to develop better human beings who derive greater fulfillment from the ‘other.’⁵⁸

In boiling down the purpose of intervention to stopping mass murder, “nothing more and nothing less,” Professor Glennon ignores the reality that intervention invariably creates local vacuums of power and purpose which will likely fill with only more suffering if absolutely no effort is made to preserve the peace and build something from the ashes.

CONCLUSIONS

The military would probably be the first to agree that nation building is not a mission it traditionally embraces.⁵⁹ But without substantial military

⁵⁷ BOB WOODWARD, PLAN OF ATTACK 150 (2004) (attributing to National Security Advisor Colin Powell the voicing of this cautionary principle in discussions leading up to the invasion of Iraq).

⁵⁸ Michael J. Glennon, *American Hegemony in an Unplanned World Order*, 5 J. CONFLICT & SECURITY L. 3, 24 (2000).

⁵⁹ The military acronym “MOOTW” stands for Military Operations Other Than War and encompasses non-combat missions such as nation building and peacekeeping. JOINT CHIEFS OF STAFF, JOINT PUB. 3-07, JOINT DOCTRINE FOR MILITARY OPERATIONS OTHER THAN WAR, at vii-x (16 June 1995). Many in the military like to quip that MOOTW actually stands for “More Operations Other Than What I signed up for.”

protective assistance, the weak internal HN security situation (from degraded national military assets to ineffective local police and courts) in the wake of initial interventions would leave non-government organizations too vulnerable to be effective at assisting with rebuilding. Thus, if we must use shock and awe to get us through the front door, then we must be prepared to punch the clock and uphold the law until an interim HN government can sufficiently establish itself to run its own affairs. These are typically not short engagements, and there are no shortcuts without consequences.⁶⁰

Despite the challenge, a positive and lasting difference is possible. In Iraq, Islamic thought and Arab culture are not incompatible with the development of democracy.⁶¹ However, cutting and pasting together constitutions and codes of law from the West and expecting foreign populations and governmental institutions to gratefully step up and fall in line is both demeaning and unrealistic. Globally, non-Western cultures cannot be shocked and awed into a new world order by countries that initially intervene for humanitarian reasons but then linger to legitimately ensure the peace lasts longer than the moment after withdrawal. The “six thresholds” and the “three pillars” are certainly useful concepts to continue the dialogue about the form R2P should take. Regardless of the specific manifestation of R2P, heads of state and diplomats who seek solutions to HR abuses, just like Commanding Officers faced with surprisingly similar issues at localized levels, must develop extreme patience, keen cultural awareness, and tremendous self-restraint to establish a workable doctrine that effectively deters violations of human rights and still preserves a foundation on which to continue to build relationships.

⁶⁰ “[T]he emergence of the rule of law is a lengthy historical process linked to cultural or economic transformations. In this view, hasty efforts to foster the rule of law in only a few years are futile, especially in poor, ethnically divided societies with low degrees of institutionalization.” Charles T. Call, *Introduction: What We Know and Don’t Know about Postconflict Justice and Security Reform* in CONSTRUCTING JUSTICE AND SECURITY AFTER WAR 3, 10 (Charles T. Call ed., 2007).

⁶¹ Lawrence Rosen, *Expecting the Unexpected: Cultural Components of Arab Governance*, ANNALS AM. ACAD. POL. & SOC. SCI., Jan. 2006, at 163, 177.

THE LIMITS OF POWER: THE END OF AMERICAN EXCEPTIONALISM¹

Major Scott A. DiRocco²

*Get thine house in order.*³

I. INTRODUCTION

Starting with the quote on the publisher's page, Andrew Bacevich sets the tone for his latest book. In *The Limits of Power: The End of American Exceptionalism*, Bacevich diagnoses what ails the United States, individually and collectively, and explains how those shortcomings are reducing our international standing and power. It is a warning that America must view itself, and its place in the world, objectively. If not, we will lose the ability to chart our own destiny.

American Exceptionalism refers to the theory that America has a "uniqueness of character and purpose" among nations in various aspects from government to religion to democracy.⁴ It is this belief in our exceptionalism, Bacevich argues, that our leaders have relied upon to attempt to exercise hegemony over the world and reshape it in our image. Today, however, in the midst of an eight-year "global war on terror" with no end in sight, this belief in our exceptionalism threatens to erode our national power.

Bacevich's background alone demands attention. A 1969 graduate of West Point, Bacevich served in the Army for over 20 years before retiring as a Colonel in the early 1990s. Following his distinguished military career, Bacevich earned a Ph.D. in American Diplomatic Relations from Princeton University. He was a professor at West Point and Johns Hopkins before moving to Boston University in 1998.⁵

Bacevich organizes his assessment of America into three crises: the crisis of profligacy, the political crisis, and the military crisis. Covering each one equally, Bacevich gives us a well researched and introspective appraisal of ourselves.

¹ ANDREW J. BACEVICH, *THE LIMITS OF POWER: THE END OF AMERICAN EXCEPTIONALISM* (2008).

² Judge Advocate, U.S. Army. Student, 58th Judge Advocate Officer Graduate Course, The Judge Advocate General's Legal Ctr. & Sch., U.S. Army, Charlottesville, Va.

³ BACEVICH, *supra* note 1, at publisher's page (quoting 2 *Kings* 20:1).

⁴ BACEVICH, *supra* note 1, at 18.

⁵ See Andrew J. Bacevich—Biography, <http://www.bu.edu/ir/faculty/bacevich.html>.

II. CRISIS OF PROFLIGACY

*A world that once indulged American profligacy is no longer willing to do so. ...To preserve that which we value most in the American way of life, therefore, requires modifying that way of life, discriminating between things that are essential and those that are not.*⁶

None of Bacevich's crises involve the American individual more than the crisis of profligacy. In fact, our ethic of self-indulgence and gratification drive the other two. Bacevich's thesis is readily apparent: American excess has caused a dependency on foreign goods (especially oil), cheap labor, and credit that has negatively shaped our foreign policy. It is this self-gratification that Bacevich contends threatens our way of life and has saddled us with costly commitments abroad that we are increasingly ill-equipped to sustain.⁷

Bacevich traces our profligacy back to the end of World War II when the U.S. was a true hegemon. The U.S. was an industrial and manufacturing giant with no equals. With this economic power came freedom. According to Bacevich, Americans started to define freedom in a materialistic way as the freedom to have whatever we want, far from the definition of freedom that our forefathers envisioned.⁸

But economic power was no longer a sure way to exert our will when our imports surpassed our exports during the Vietnam War.⁹ In order to keep up with our individual demands, especially our growing dependence on foreign oil, the government increased its reliance on hard power as a way to keep foreign markets open to our consumers. Bacevich argues that, despite what we may think of our country, we have always been a country of expansion. When the borders couldn't satisfy our needs, we simply pushed them out.¹⁰ Our current forays into the Middle East should come as no surprise.

Of interest and crucial to the progression of his theme, Bacevich discusses President Jimmy Carter's "Malaise" speech¹¹ and Ronald Reagan's

⁶ BACEVICH, *supra* note 1, at 189.

⁷ *Id.* at 17.

⁸ *Id.* at 22-24.

⁹ *Id.* at 29.

¹⁰ *Id.* at 20.

¹¹ Of note, President Carter never used the word "malaise" in his speech. BACEVICH, *supra* note 1, at 35. See also Jimmy Carter, President, U.S.A., Televised Address: The Crisis of Confidence (July 15, 1979), available at http://www.pbs.org/wgbh/amex/carter/filmmore/ps_crisis.html.

response.¹² In his speech, which was given in the midst of the 1979 energy crisis, President Carter told the American people that he could not fix the problem alone; they would have to curb their appetites and search within themselves to find out what was truly important to them.¹³ In response to this attempt to curb America's unchecked consumerism, Reagan labeled President Carter a pessimist and discounted the notion that America had to "learn to live with less."¹⁴ One year later, Reagan won in a landslide. Bacevich points to this moment as the last time a politician could ask the American people to limit themselves and, in doing so, points out a bridge between America's self-indulgence and the actions of its elected politicians. In the end, he asserts that America's leaders "have proven unable (or unwilling) to address the disparity between what we want and how much we can afford to pay."¹⁵

III. THE POLITICAL CRISIS

*Efforts to identify the lessons to be learned from that catastrophe [Iraq] have focused on operational matters...Yet this preoccupation with tactics and operations diverts attention from the far more critical failings in the realm of politics.*¹⁶

To Bacevich, the political crisis goes far beyond the errors in judgment by the executive branch that culminated with the second Bush administration. In his view, we all caused the crisis, from the legislature that willingly yielded its power and authority, to the executive,¹⁷ to the civilian advisors of the President who have consistently promoted an increasingly militaristic and imperial foreign policy, to the American people who continue to underwrite the entire failing government.

According to Bacevich, the national security policies that were conceived during World War II and continue through today now endanger the very country that they were created to protect.¹⁸ Starting in 1949 with the Soviet Union's first atom bomb detonation and China's communist revolution and proceeding through every major foreign policy conflict, Bacevich details how

¹² BACEVICH, *supra* note 1, at 36-37.

¹³ Interestingly, President Carter's speech is quite conservative as defined by today's norms. *See generally* Carter, *supra* note 11.

¹⁴ Ronald Reagan, Candidate for President, U.S.A., Official Announcement of his Candidacy for President (November 13, 1979), available at <http://www.4president.org/speeches/reagan1980announcement.htm>.

¹⁵ BACEVICH, *supra* note 1, at 10.

¹⁶ *Id.* at 121.

¹⁷ *Id.* at 69.

¹⁸ *Id.* at 72.

our government has overestimated the threat from perceived national security crises and relied on the militaristic response on an ever growing magnitude. Soft power, whether in the form of diplomacy, economic health, or morality, has ceded its place to hard power as a response to political crises.

To support this ideology of national security, the government has created a huge national security apparatus.¹⁹ Far from protecting the national security of our country, Bacevich contends that these agencies and their policies continually fail, setting our country up for future conflicts.

Relying on a wealth of source material, Bacevich details how civilian advisors to the President, whom he sarcastically calls “wise men,” have shaped our national security policies since World War II. Men such as James Forrestal, Paul Nitze, and Paul Wolfowitz have consistently promoted the national security agenda and pushed our country further down the path towards militaristic imperialism. Bacevich sagely points out that most of these wise men are personnel who retired from the national security apparatus and have a vested interest in maintaining it.²⁰

Although Bacevich is a harsh critic of the Bush Administration and its foreign policy decisions, he gains credibility in this section by pointing out that Bush did not create a grand new foreign policy as his supporters and detractors both suggest. According to Bacevich, Bush simply reaffirmed the U.S.’s ideology of national security “to which past administrations have long subscribed.”²¹ Bacevich urges us to look past the “superficial differences” between the parties and notice the “subterranean similarities” which really matter.²²

Bacevich’s appraisal of the legislative branch is equally acerbic. While he lambastes the executive branch for its imperial and militaristic policies, he equally chides the legislature for willfully letting it happen. Since World War II, the legislature has consistently yielded its power and authority to the executive branch. According to Bacevich, Congress is concerned more with getting itself reelected than standing up to the power-hungry executive.²³ As a result, Bacevich surmises, we are stuck with an executive that continues foreign

¹⁹ This bureaucracy includes the State Department, the Office of the Secretary of Defense, the armed services, various intelligence agencies, the Joint Chiefs of Staff, the National Security Council, and the FBI. *Id.* at 72.

²⁰ President Obama’s current cabinet is a perfect example. See BACEVICH, *supra* note 1, at 186.

²¹ With that said, Bacevich asserts that Bush articulated this ideology “with such fervor and clarity as to unmask as never before its defects and utter perversity.” *Id.* at 74.

²² *Id.* at 74.

²³ *Id.* at 69.

policies that decrease our influence and power and a legislature too weak to stop it.

IV. THE MILITARY CRISIS

*America doesn't need a bigger army. It needs a smaller—that is, more modest—foreign policy, one that assigns soldiers missions that are consistent with their capabilities.*²⁴

With the politicians increasing use of hard power to help satisfy the American appetite for foreign oil and goods, you would think that our military would be invincible. That's what our government tells us, anyway. Bacevich says to think again. In his opinion, as measured by results achieved, the military is unimpressive²⁵ and we are not getting a return on our substantial annual investment.

Central to his argument is the fact that our Presidents and senior military officials have forsaken strategy for ideology as a means to an end and, in the process, entered us into two wars that cannot be maintained and are likely unwinnable by our all-volunteer force. This despite the fact that history has shown that war is anything but certain.²⁶ To persist down this path believing that we have somehow mastered the art of war, Bacevich argues, “invites overextension, bankruptcy and ruin.”²⁷

Bacevich details the ineptitude of our senior military officers with an especially caustic assessment of General Tommy Franks, military architect of both the Iraq and Afghanistan invasions. He finds fault with the country's eagerness to use the military to solve most diplomatic issues and condemns the government's exaggeration of our military might.

Bacevich is quick to point out that it's not the individual Soldiers or units who are failing. To the contrary, he maintains that the “problem lies less with the Army that we have—a very fine one, which every citizen should wish to preserve—than with the requirements that we have imposed on our soldiers.”²⁸

Bacevich asserts that preventative war is immoral and unjust and never the answer to political problems. An outspoken and constant critic of the Bush

²⁴ *Id.* at 169.

²⁵ BACEVICH, *supra* note 1, at 169.

²⁶ Bacevich aptly quotes Churchill on this point: “The statesman who yields to war fever is no longer the master of policy, but the slave of unforeseeable and uncontrollable events.” *Id.* at 157 (quoting WINSTON CHURCHILL, *MY EARLY LIFE* 232 (Simon & Schuster 1996) (1930)).

²⁷ BACEVICH, *supra* note 1, at 169.

²⁸ *Id.* at 169.

administration's "global war on terror," Bacevich has also personally felt the consequences of this policy. On 13 May 2007, his son, First Lieutenant Andrew Bacevich, Jr., was killed by an improvised explosive device while serving in Iraq.²⁹ To Bacevich's credit, he does not allow the reader to know of his son's death until the Acknowledgments. Any attempt to marginalize his position as the product of a bitter parent who has lost a child is misplaced. Bacevich's stance on our country's foreign policy pre-dates the death of his son.³⁰

V. BACEVICH'S PROPOSED ALTERNATIVES

In the end, Bacevich offers a few alternatives to our country's current global war on terror. Bacevich proposes using the strategy of containment to combat violent Islamic extremism.³¹ The purpose of containment today, Bacevich argues, would be to contain the influence of radical Islam. As with the Cold War where it was successful, a strategy of containment would allow Radical Islam to show its deficiencies without letting it infringe into our country.

He also argues that we should completely dismantle our nuclear arsenal. In his view, nuclear weapons are unusable; their deployment would be a "moral and political catastrophe."³² Their very existence, moreover, makes our position against proliferation hypocritical and encourages our current enemies to obtain them to counter our threat.³³

Preserving our planet should be a priority, Bacevich further asserts, and goes hand in hand with the reduction of fossil fuel use. Transforming mankind's relationship with our environment, he sardonically reasons, could hardly be more difficult than transforming the way of thinking of a billion Muslims in the Greater Middle East.³⁴

Most radical of all, Bacevich proposes dismantling most of the national security apparatus. The trillions of dollars we spend on it, he contends, could be put to better use. Even using those funds to research alternatives to fossil fuel would have a greater impact on our national security than we've received over the past 40 years.³⁵

²⁹ *Id.* at 203.

³⁰ For an example, see Andrew J. Bacevich, *Rescinding the Bush Doctrine*, Boston Globe, March 1, 2007, available at http://www.boston.com/news/globe/editorial_opinion/oped/articles/2007/03/01/rescinding_the_bush_doctrine/, published two months before the passing of his son.

³¹ BACEVICH, *supra* note 1, at 176.

³² *Id.* at 178-79.

³³ *Id.* at 179.

³⁴ *Id.* at 180.

³⁵ *Id.* at 180-81.

VI. CONCLUSION

The Limits of Power is packed with scholarly research, sound arguments, and considered opinions. Yet it is Bacevich's smooth writing style that allows the reader with little or no prior understanding of this subject to follow his arguments and propositions. Very few authors have given such an unfettered and clear critique of American policy in so few words. It is this writing style that raises this book above others.

The book is not without its limitations, however. One of its glaring holes is Bacevich's proposed solution, or lack thereof, to the crisis of profligacy. Bacevich simply does not articulate a way forward for the individual or country as a whole. The best the reader can surmise from Bacevich is simply to learn to live with less. This void falls short, especially when following such a detailed and eloquent discussion of our internal problems.

While Bacevich does an exceptional job of advocating for the strategy of containment as a better way to handle radical Islam, larger domestic questions remain unanswered. How do we curb our dependence on foreign goods, oil, and credit? How do we deal with our foreign debt? How do we, the American people, hold our elected officials responsible for their actions? How do we dismantle the national security apparatus? How will the new defense structure be organized? How long will this transformation take? Maybe detailing the way ahead is a topic for another book; it would certainly add considerably to the length of this work. But Bacevich's clear assessment of our country's failings grabs your attention and begs the question, "OK, what next?" – a question he fails to adequately answer.

Bacevich does depart from his overall clear and succinct style with his repeated referrals to Reinhold Niebuhr, a twentieth century theologian who was known for applying the doctrines of Christianity to the real world.³⁶ While each Niebuhr quote that Bacevich cites is relevant to Bacevich's overall theme of the consequences of American self-indulgence and hypocrisy, the recurring references³⁷ contrast with Bacevich's otherwise clear prose. You get the feeling as a reader that Bacevich comingled his personal fondness for Niebuhr's

³⁶ See RONALD H. STONE, PROFESSOR REINHOLD NIEBUHR: A MENTOR TO THE TWENTIETH CENTURY 60-89 (1992).

³⁷ By my count, Bacevich refers to Niebuhr on 15 pages, some with multiple quotes. See BACEVICH, *supra* note 1, at 6, 7, 9, 12, 23, 42, 49, 68, 81, 119, 122, 164, 174, 182, and 188.

writings with the overall task of this book.³⁸ As Bacevich did such an exceptional job of making sure that his book could be grasped by an audience with no formal background in history or political science, the repeated references to this iconic intellectual distract from the main theme of the book and add little to Bacevich's otherwise strong position.

The Limits of Power should be mandatory reading for all military officers. It is an abrasive, almost painful, review of our storied profession. But if the officer can get past the superficial sting of Bacevich's assessment, he or she has the opportunity to learn the actual capabilities, and limits, of our military power. Our civilian leadership will reap the gains. The true value of Bacevich's critique, though, is saved for our policy makers and elected officials. They are the ones with the ability to use this book as a way forward for American policy into the 21st century.

All in all, *The Limits of Power* is a must-read for anyone who cares deeply about the future of America. Bacevich delivers a wake-up call that everyone can digest. Ultimately, Bacevich feels that we are a hypocritical nation in denial.³⁹ Hypocrisy breeds a lack of self awareness which leads to colossal errors in judgment. Only by objectively reevaluating ourselves, both individually and collectively, can we start to right the ship. I eagerly await his next book on how we get there.

³⁸ Bacevich authored the introduction to one of Niebuhr's recently republished books, calling it the "most important book ever written on U.S. policy." Andrew J. Bacevich, *Introduction* to REINHOLD NIEBUHR, *THE IRONY OF AMERICAN HISTORY*, ix (U. Chi. Press Ed. 2008) (1952). Bacevich also referred to Niebuhr as "the most clear-eyed of American prophets." BACEVICH, *supra* note 1, at 6.

³⁹ BACEVICH, *supra* note 1, at 181.

WIRED FOR WAR: THE ROBOTICS REVOLUTION AND CONFLICT IN THE 21ST CENTURY¹

Major Robert A. Rodrigues²

*A robot may not injure a human being, or, through inaction, allow a human being to come to harm.*³

I. INTRODUCTION

In *Wired for War*, P.W. Singer describes the coming “Robotics Revolution”⁴ and its impact on the battlefield of today and the near future. Singer examines current and emerging military robotic and unmanned systems technology, along with the corresponding social, political, and strategic implications raised by the use of such weapons. *Wired for War* essentially serves as a roadmap for where this technology is taking us, and the many obstacles we must overcome to reach a desirable destination.

II. ORGANIZATION AND CONTENT

Wired for War is an ambitious attempt to analyze the present effects and foreseeable consequences of deploying robotic and unmanned systems on the battlefield from almost every conceivable angle. To accomplish this, Singer relies primarily on input from the highest and lowest levels of the chain of command, human rights organizations, and private defense contractors for assistance in framing the issues.⁵ Recognizing the difficulty of making predictions based on theoretical technological advances, Singer wisely limits his analysis to currently available systems or those already under development.⁶

¹ P.W. SINGER, WIRED FOR WAR: THE ROBOTICS REVOLUTION AND CONFLICT IN THE 21ST CENTURY (2009).

² Judge Advocate, U.S. Army. Student, 58th Judge Advocate Officer Graduate Course, The Judge Advocate Gen.’s Legal Ctr. & Sch., U.S. Army, Charlottesville, Va.

³ The Three Laws of Robotics are:

1. A robot may not injure a human being, or, through inaction, allow a human being to come to harm. 2. A robot must obey the orders given it by human beings except where such orders would conflict with the First Law. 3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

See e.g., ISAAC ASIMOV, I, ROBOT (1950).

⁴ SINGER, *supra* note 1, at front cover.

⁵ *Id.*

⁶ *Id.* at 14.

Singer begins his book by chronicling the rapid rise of robotic and unmanned systems in Iraq since 2003.⁷ He identifies two main types of systems currently in use. The first are ground-based robots in Iraq and Afghanistan, such as the lawn mower-sized PackBot, which is used primarily to defuse Improvised Explosive Devices (“IEDs”).⁸ The second are air drones such as the Predator Unmanned Aerial Vehicle (“UAV”), frequently controlled remotely by pilots in the United States.⁹

To put the current state of technology in context, Singer identifies three main reasons for the recent rise in unmanned systems. The first is the expectation of low casualties in the wake of Desert Storm.¹⁰ Second, he chronicles mandates from Congress to the Department of Defense to incorporate unmanned systems.¹¹ Lastly, he identifies the terrorist attacks of 11 September 2001 as the main catalyst for unmanned system development.¹²

Singer also looks to the near future and identifies a number of systems currently under development. He notes that the current trend is to create larger robots and UAVs that carry more and larger weapons, such as the next generation UAV, the Reaper.¹³ On the ground, he highlights the Modular Advanced Armed Robotic System (MAARS), which is similar to the IED-defusing PackBot, but augmented with offensive weapons such as a machine gun and 40mm grenade launcher.¹⁴

Singer then analyzes the strategic, social, and political implications that come with the development and use of these systems. He hypothesizes that robotic and unmanned systems may demoralize our enemy to the point of surrender because they can’t kill flesh-and-blood Soldiers.¹⁵ Singer worries, however, that reliance on unmanned systems when fighting an insurgency may serve to strengthen our enemies’ resolve because this reliance may be viewed as a sign of weakness and lack of courage.¹⁶ In a worst-case scenario, Singer warns

⁷ The number of robots in Iraq rose from zero in 2003 to 12,000 in 2008. *See Id.* at 32.

⁸ *Id.* at 22.

⁹ As of 2008, there were 28 different robot systems operating on the ground in Iraq. By 2008 there were 5,331 drones in the U.S. Air Force inventory; almost double the amount of manned planes. *See SINGER, supra* note 1, at 32, 37.

¹⁰ *Id.* at 59.

¹¹ *Id.*

¹² *Id.* at 61.

¹³ *Id.* at 111, 116.

¹⁴ *SINGER, supra* note 1, at 111.

¹⁵ *Id.* at 298.

¹⁶ *Id.* at 309.

that if our technology advances to the point of invincibility, it may discourage direct conflict and instead encourage strikes at our civilian population centers.¹⁷

Singer examines a potential unintended political consequence that the proliferation of this technology may produce. With less and less risk to human life on the battlefield, he worries that governments may find it increasingly attractive to resort to armed conflict as a means of advancing their nation's interests.¹⁸

Singer also identifies a number of practical challenges brought about by the use of robotic and unmanned systems. First, he points out the fact that technology is outpacing military doctrine regarding how to integrate these systems into our current force structure.¹⁹ Second, he notes that no logistics are in place in Iraq and Afghanistan for servicing these systems.²⁰ Singer also notes the effect that these systems have had on military culture and command structure, particularly in the case of the Air Force, where he describes nineteen-year-old video game geeks as quickly replacing veteran pilots as its most important human asset.²¹

Of particular note to Judge Advocates, Singer conducts a fairly extensive examination of the Law of War ("LOW") implications raised by these systems. Singer's basic premise is that the current LOW is not able to adequately address the issues raised by these new technologies and that no group is actively seeking to remedy the situation. On the one hand, he feels that machines are less likely to commit LOW violations since they do not have human emotions.²² At the same time, however, he worries that this lack of emotion may allow machines to engage in indiscriminate killing that a human would otherwise avoid.²³

Singer recognizes the difficulty in fixing responsibility for LOW violations committed by these systems. For example, if a system wrongfully kills a civilian, Singer questions where ultimate responsibility should rest, be it with the manufacturer, software engineer, buyer, or user of the system.²⁴ Singer believes that a commander could be found criminally liable if he did not take proper precautions when using a system.²⁵ More controversially, he believes that

¹⁷ *Id.* at 312.

¹⁸ *Id.* at 316.

¹⁹ SINGER, *supra* note 1, at 208.

²⁰ *Id.* at 211.

²¹ *Id.* at 361.

²² *Id.* at 393.

²³ *Id.* at 396.

²⁴ SINGER, *supra* note 1, at 389.

²⁵ *Id.* at 411.

a system creator could be found criminally liable for its product's bad acts by analogizing to product liability laws.²⁶

Singer goes so far as to suggest that robots may eventually be recognized as having an inherent right of self defense, which creates an entirely separate set of legal concerns.²⁷ In order to avoid many of these difficult issues, Singer offers one possible solution, namely, restricting autonomous systems to only nonlethal force and requiring human input to use lethal force. This solution would ensure that a flesh-and-blood human would still be legally responsible for any LOW violations.²⁸

III. ANALYSIS

Wired for War provides the reader with a thorough overview of the implications of fielding robotic and autonomous systems on the battlefield. Despite the obvious technical nature of the subject matter, Singer purposely frames his book to avoid alienating potential readers by getting bogged down in technical lingo.²⁹ As a result, the book is clear and accessible to any reader, regardless of his prior understanding of robot technology.

The breadth of Singer's work is truly impressive. He makes an ambitious effort to examine his subject from the first hand perspectives of those most affected by this technology. He considers the implications of these systems on the Soldier with the remote control or joystick in his hand, the commanders, the government employing the systems, the companies developing them, and even our enemies facing these systems. As a result, the reader is exposed to multiple, often competing interests. Unfortunately, Singer draws most of the book's main points from his interviews rather than offering his own analysis or conclusions. As a result, the reader is frequently left with more questions than answers.

One group conspicuously absent from Singer's broad spectrum of players is the Judge Advocate ("JA"). In fact, he devotes no more than five sentences in his entire book to the military legal community. Whether this exclusion was purposeful or merely an oversight, the effect on Singer's analysis of the legal issues is obvious. His conclusions are hampered by a number of legally inaccurate premises. For example, when discussing civilian contractor responsibility for war crimes, he states that civilians should not be allowed to

²⁶ *Id.* at 410.

²⁷ *Id.* at 406.

²⁸ *Id.* at 409.

²⁹ SINGER, *supra* note 1, at 12.

control unmanned systems because the military can't court-martial civilians.³⁰ This is not correct, as the Uniform Code of Military Justice was amended in 2006 (*Wired for War* was published in 2009) to grant jurisdiction over persons serving with or accompanying an armed force in the field during a time of declared war or contingency operation.³¹ Furthermore, Singer makes no mention of the Military Extraterritorial Jurisdiction Act of 2000, which would provide another means of prosecuting civilian contractors.³²

Singer's analysis of civilian contractors on the battlefield continues to suffer as he worries they may be considered illegal combatants like "al-Qaeda detainees" instead of the traditional classification of noncombatants.³³ The concept of a civilian accompanying the force, which appears to be the most logical classification, does not enter Singer's analysis.

One of Singer's main points is that the current law of war structure, primarily the Geneva Conventions, is not equipped to deal with these systems. As a result, Singer attempts to paint a picture of almost complete legal confusion regarding these systems.³⁴ Singer focuses almost exclusively on the International Committee of the Red Cross ("ICRC") as being responsible for defining and defending the law of war.³⁵ He specifically notes that no one interviewed for his book mentioned the ICRC and its four pillars of international humanitarian law on weapons as evidence of this vast legal confusion.³⁶ Curiously, Singer's search for applicable guidelines in this area stops short of making any discernible attempt to determine what the current Rules of Engagement ("ROE") are regarding the use of robotic or unmanned systems. While it is possible that such ROE would not be printable due to its classification status, the fact that Singer does not ask any current commanders what the ROE is or even refer to its existence reflects a either a deliberate omission or lack of understanding of how the military places legal constraints on Soldiers.

Unfortunately, Singer's misunderstanding of the law is evident throughout the book. For instance, he confuses the concepts of *jus in bello* and *jus ad bellum* when giving a definition of "proportionality."³⁷ Most seriously,

³⁰ *Id.* at 408.

³¹ See UCMJ art. 2 (2008) (providing for court-martial jurisdiction over persons serving with or accompanying an armed force in the field in a time of declared war or contingency operation).

³² See generally Military Extraterritorial Jurisdiction Act, 18 U.S.C. §§ 3261-3267 (2000) (providing for prosecution of civilians in federal court for crimes committed while accompanying the force outside the U.S.)

³³ SINGER, *supra* note 1, at 372.

³⁴ *Id.* at 386.

³⁵ *Id.* at 384.

³⁶ *Id.* at 385.

³⁷ *Id.* at 383. Singer incorrectly states that the *jus in bello* concept of proportionality relates to the decision to go to war. In fact, *jus in bello* proportionality relates to the proper amount of force used

when discussing the potential right of unmanned drones such as UAVs to defend themselves, Singer states that current Air Force policy is that UAVs are “national property” and are considered representatives of the United States, and thus have the same right of self-defense as a person.³⁸ Singer cites a 2001 Air Force Law Review article for this controversial premise.³⁹ A review of the article, which deals with the integration of JAs and paralegals in Air Force operations, reveals that it contains no mention or analysis of the classification of UAVs or the defense of such systems.⁴⁰ Whether this is simply an attribution error or a deliberate misrepresentation, such incongruity taints Singer’s analysis and reveals the dangers of failing to engage the subject matter experts, in this case military lawyers, when discussing the LOW.

IV. LESSONS FOR JUDGE ADVOCATES

Wired for War raises a number of short and long term issues that JAs will need to address regarding these systems. The most immediate concern is the need for JAs to familiarize themselves with the robotic and unmanned systems currently in use and identify the legal issues raised by such use. One researcher has even suggested that legal oversight should begin during the development of these systems rather than waiting for them to be deployed.⁴¹

Judge Advocates must be able to advise Soldiers and commanders on the proper use of these systems and determine who is responsible when a mistake is made. Depending on the type of system, this can be more difficult than it appears. In the case of systems such as the Unmanned Combat Aerial Vehicle (“UCAV”), the Soldier controlling the system may not even fall under the chain of command of the commander who has called for UCAV support. If the UCAV shoots a civilian, it seems logical that the “pilot” bears responsibility, but what about the commander watching the engagement unfold on his computer screen? If he does not intervene, does he bear responsibility as well?

This question becomes even more difficult when a fully autonomous system (with no human control) mistakenly kills a civilian. The consensus among most commentators is that the commander who ordered the deployment of the weapon would be held responsible for the consequences of its use.⁴² If a

once in war, while *jus ad bellum* proportionality relates to the decision to go to war. See, e.g., ALEXANDER MOSELEY, JUST WAR THEORY, at <http://www.utm.edu/research/iep/j/justwar.htm>.

³⁸ SINGER, *supra* note 1, at 407.

³⁹ *Id.* at 480.

⁴⁰ See Colonel Charles Dunlap, *The Revolution in Military Legal Affairs: Air Force Legal Professionals in 21st Century Conflicts*, 51 A.F. L. REV. 293, 293-309 (2001).

⁴¹ Anthony Finn, *Legal Considerations for the Weaponization of Unmanned Ground Vehicles*, 1 INT. J. INTELLIGENT DEF. SUPPORT SYSTEMS 43, 50 (2008).

⁴² SINGER, *supra* note 1, at 48.

system malfunctions due to a software glitch and kills a civilian, however, it seems unfair for a commander to bear responsibility for what is essentially a product defect. This raises the obvious question of whether a system developer should be held liable for its creation's actions under a product liability theory. Such a threat of creator liability would undoubtedly curb future development of lethal autonomous systems.

The use of robot and unmanned systems, particularly autonomous ones, will necessitate the creation of specific legal rules to govern their use on the battlefield. Whether this can be done solely through implementing specific ROE remains to be seen. Teaching ROE to human beings is difficult enough. Successfully programming these rules into a computer program so that a robot can discriminate between an insurgent with a Rocket Propelled Grenade and a farmer with a shovel is regarded as incredibly difficult, if not impossible, by many researchers.⁴³ Others, however, believe it may be possible for robots to follow ROE with the assistance of human inputs on a mission-specific basis.⁴⁴ Once a feasible means of programming ROE into a computer is achieved, robotic and unmanned systems may have to be validated as ROE-compliant before being deployed in combat. Judge Advocates may be required to assist in the development of scenarios that form the basis of this validation process.

Depending on their proliferation and capabilities, these systems may ultimately require an international treaty to define permissible and impermissible uses. Like any controversial weapon, it is likely that countries with advanced robotics will favor fewer restrictions than those countries with less advanced systems. The aforementioned validation process will likely be crucial to gaining international acceptance of these systems.

V. CONCLUSION

The future of combat likely lies in robot and unmanned systems. *Wired for War* is a comprehensive introduction to the numerous tactical, social, and legal issues raised by the use of these systems. We are only beginning to feel the effects of what is likely to be a fundamental change in the way that wars are fought. Singer's book provides an insightful though somewhat flawed attempt to highlight the challenges for the military to effectively employ this emerging technology while managing to retain its traditional command structure and values, all while conforming to the LOW.

⁴³ *Id.* at 76.

⁴⁴ See e.g., RONALD C. ARKIN ET AL., RESPONSIBILITY AND LETHALITY FOR UNMANNED SYSTEMS: ETHICAL PRE-MISSION RESPONSIBILITY ADVISEMENT, TECHNICAL REPORT GIT-GVU-09-01 (2007), at <http://www.gvu.gatech.edu/reports/09-01.pdf>.

The continuously evolving nature of technology means that the systems described in *Wired for War* could be obsolete in a few years. Singer's concerns, however, will likely persist until the military, particularly its legal community, comes to grips with either trying to shoehorn these systems into existing legal concepts or by creating new laws to govern their use. In this regard, *Wired for War* is a thought-provoking book that any military law practitioner would be well advised to read in preparation for meeting these inevitable challenges.

INFORMATION FOR AUTHORS

Authors are invited to discuss prospective articles with the NAVAL LAW REVIEW Editor-in-Chief at (401) 841-3800 ext. 141 or DSN 841-3800 ext. 141 or by writing to Editor-in-Chief, NAVAL LAW REVIEW, Naval Justice School, 360 Elliot Street, Newport, RI 02841-1523 or via e-mail at: Naval_Law_Review@navy.mil.

The Editor-in-Chief, in conjunction with article editors, carefully reviews each manuscript for clarity, accuracy, and scholarly merit. The Editor-in-Chief reserves the right to make editorial changes to a manuscript selected for publication. Manuscripts will not normally be altered in a manner inconsistent with the substance of the author's position. Where practical, the board will notify the author of any substantive changes before publication. There are no specific guidelines on manuscript length: brevity is not an obstacle to publication of a quality manuscript.

Manuscripts must be submitted in Microsoft Word 2003 format. Authors should include an abstract of the proposed article, a short biography, and a statement as to whether the manuscript has been submitted elsewhere for publication. Per current directives, authors are solely responsible for security review. Authors may take a different position from that held by the government; when the author purports to state the views of the Department of the Navy or another governmental entity, however, security review is essential to ensure that the official position is stated accurately. No compensation can be paid for any articles published.

Articles should conform to the current edition of *A Uniform System of Citation* (18th ed.) and *Military Citation* (7th ed.). Authors should consult the *United States Government Printing Office Style Manual* (rev. ed. 1984), on matters not addressed in *A Uniform System of Citation* ("The Bluebook").